

Chapter 3

Congruence

Introduction

It is curious how often seemingly very different branches of mathematics become interlinked by some problem. For more than 2000 years it had been known how to construct both an equilateral triangle and a regular pentagon inscribed in a given circle using only compass and straight edge. But as the seventeenth century drew to its close, constructions were still not known for any other regular polygon with a prime number of sides. The brilliant French mathematician Fermat had been discussing the numbers $F_n = 2^{2^n} + 1$ (later to become known as *Fermat numbers*), believing them all to be prime, unaware of how intricately these numbers were woven into the solution of the polygon problem. It required the genius of the German mathematician Gauss to see how these numbers could be used to solve the construction problem.

You will learn more about Fermat in Chapter 4.

In the final section of the previous chapter we introduced the idea of a remainder sequence, in which numbers were replaced by their remainder on dividing by some natural number n . Observations about the behaviour of the remainder sequence were then projected back to reveal properties of the original number sequence. Gauss used this idea to develop an ‘arithmetic of remainders’, which he then put to work to ease computations in many areas.

You may like to read more about Gauss in the *History Reader* for this topic.

In this chapter we introduce Gauss’s notion of congruence and develop properties of it that will be useful in problem-solving throughout the remainder of the topic. Here we restrict its application to a variety of problems involving remainders and, in particular, to solving linear congruences (which offer a more general way of looking at linear Diophantine equations). Finally, we prove the classical *Chinese Remainder Theorem*, which is concerned with the existence of (and how to find) solutions to a class of problems that can be modelled as a simultaneous system of linear congruences.

Chapter guide

This chapter is set out in four sections, the most substantial of which is the first. Section 2 is the shortest, and is also not used by the final two sections.

1 Properties of congruence

This chapter begins by defining congruence, and establishing some elementary properties that will enable us to carry out basic algebraic manipulations in this setting.

1.1 Definition and basic properties

It has been suggested that the result that p divides $2^{p-1} - 1$, for every odd prime p , was known to Chinese mathematicians over 2000 years ago. But how does one go about confirming instances of this result? If asked to show that $2^{16} - 1$ is divisible by 17 it would be feasible to compute 2^{16} by hand, subtract 1, and then carefully divide by 17. But it would be impractical to try the same line of attack to confirm that 641 divides $2^{640} - 1$ because this number is so huge. You will see in this section that such divisions need not be as frightening as they first seem; we can investigate divisibility without having to do the computations involved in the division. Instead we can use an ‘arithmetic of remainders’ in which everything hinges on the following key definition.

Definition 1.1 Congruence modulo n

Let n be a fixed natural number and let a and b be any integers. We say that a is **congruent to b modulo n** if the difference $a - b$ is divisible by n .

In symbols we write $a \equiv b \pmod{n}$.

If a is not congruent to b modulo n we say that a is **incongruent to b modulo n** and write $a \not\equiv b \pmod{n}$.

If we write $a \equiv b \pmod{n}$ it is to be understood that a and b are integers and n is a natural number, for the statement would not make sense otherwise.

To illustrate the congruence notation, consider the case of modulus $n = 11$. We have

$$3 \equiv 25 \pmod{11}, \text{ since } 3 - 25 = -22 = -2 \times 11,$$

and

$$7 \equiv -26 \pmod{11}, \text{ since } 7 - (-26) = 33 = 3 \times 11.$$

On the other hand, 12 is incongruent to 8 modulo 11, since $12 - 8 = 4$, and 4 is not a multiple of 11.

Exercise 1.1

For each of the following, decide whether the statement is true or false.

- (a) $3 \equiv 29 \pmod{8}$
- (b) $3 \equiv -29 \pmod{8}$
- (c) $63 \equiv 37 \pmod{13}$
- (d) $37 \equiv 63 \pmod{13}$
- (e) $63 \equiv 63 \pmod{37}$
- (f) $63 \not\equiv 13 \pmod{25}$

Parts (c) and (d) of Exercise 1.1 illustrate one apparent property of congruence, namely that if a is congruent to b modulo n then b is

congruent to a modulo n . Part (e) illustrates the further property that any integer is congruent to itself modulo n . These are two of a number of general properties of congruence that highlight certain similarities with ordinary equality, and which we will prove in our first result.

Theorem 1.2 *Properties of congruence*

Let n be a fixed natural number and let a, b, c and d be any integers. Then the following properties hold.

- (a) $a \equiv a \pmod{n}$.
- (b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- (c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.
- (d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.
- (e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.
- (f) If $a \equiv b \pmod{n}$ then $a^r \equiv b^r \pmod{n}$, for any integer $r \geq 1$.

Proof

- (a) $a - a = 0 = 0 \times n$, so $a \equiv a \pmod{n}$.
- (b) If $a \equiv b \pmod{n}$ then there exists an integer k such that $a - b = kn$.

Then

$$b - a = -(a - b) = (-k)n,$$

so that $b \equiv a \pmod{n}$.

- (c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then there exist integers s and t such that

$$a - b = sn \quad \text{and} \quad b - c = tn.$$

Adding these two equations gives

$$(a - b) + (b - c) = sn + tn.$$

That is,

$$a - c = (s + t)n,$$

so that $a \equiv c \pmod{n}$.

- (d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then there exist integers s and t such that

$$a - b = sn \quad \text{and} \quad c - d = tn.$$

Adding these two equations gives

$$(a + c) - (b + d) = sn + tn = (s + t)n,$$

so that

$$a + c \equiv b + d \pmod{n}.$$

- (e) With $a - b = sn$ and $c - d = tn$ as in the proof of property (d),

$$ac = (b + sn)(d + tn) = bd + n(bt + sd + stn),$$

and so

$$ac - bd = n(bt + sd + stn),$$

confirming that $ac \equiv bd \pmod{n}$.

- (f) The case $r = 1$ is trivially true. Continuing by induction, suppose the result is true for $r = k$, that is, suppose $a^k \equiv b^k \pmod{n}$ whenever $a \equiv b \pmod{n}$.

Then

$$\begin{aligned} a^{k+1} &= aa^k \equiv bb^k \pmod{n}, & \text{by property (e),} \\ &\equiv b^{k+1} \pmod{n}. \end{aligned}$$

This confirms the truth of the case $r = k + 1$ and completes the induction step. The result follows by mathematical induction. ■

The following exercise gives you an opportunity to prove some simple properties of congruence by working from the definition alone.

Exercise 1.2

Suppose that $a \equiv b \pmod{n}$ and m is an integer. Prove the following.

- (a) If $m > 0$ and m divides n then $a \equiv b \pmod{m}$.
- (b) If $m > 0$ then $ma \equiv mb \pmod{mn}$ and $ma \equiv mb \pmod{n}$.
- (c) If $d > 0$ is a common factor of a , b and n , then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.
- (d) $\text{hcf}(a, n) = \text{hcf}(b, n)$.
- (e) For any integer c , $a + c \equiv b + c \pmod{n}$.

Before developing further ideas, let us illustrate a range of problems in which properties of congruence can be exploited to ease computation.

Worked Exercise 1.3

Show that $37^{37} + 2$ is divisible by 13.

Solution

We start by looking for numbers to which 37^{37} is congruent modulo 13. Now as $37 \equiv -2 \pmod{13}$, Theorem 1.2(f) tells us that

$$37^{37} \equiv (-2)^{37} \equiv (-1) \times 2^{37} \pmod{13}.$$

Now

$$2^4 = 16 \equiv 3 \pmod{13},$$

and so

$$37^{37} \equiv (-1) \times (2^4)^9 \times 2 \equiv (-1) \times 3^9 \times 2 \pmod{13}.$$

But

$$3^3 = 27 \equiv 1 \pmod{13},$$

so

$$37^{37} \equiv 3^3 \times 3^3 \times 3^3 \times (-2) \equiv -2 \pmod{13}.$$

Finally, Theorem 1.2(d) allows us to conclude that

$$37^{37} + 2 \equiv (-2) + 2 \equiv 0 \pmod{13},$$

which amounts to saying that $37^{37} + 2$ is divisible by 13.

In the final step of Worked Exercise 1.3 we inferred from a statement of the form $a \equiv 0 \pmod{n}$ that n divides a . This is an immediate consequence of the definition of congruence. Indeed, we have a characterisation of congruence modulo n in terms of the remainders on dividing by n , as given by the following proposition.

Proposition 1.4 *Congruent integers have the same remainders*

$a \equiv b \pmod{n}$ if, and only if, the integers a and b have the same remainder when divided by n .

Proof Suppose first that a and b have the same remainder when divided by n , say

$$a = q_1n + r \quad \text{and} \quad b = q_2n + r, \quad \text{where } 0 \leq r < n.$$

Then $a - b = (q_1 - q_2)n$, showing that $a \equiv b \pmod{n}$.

Conversely, suppose that $a \equiv b \pmod{n}$, so that $a - b = kn$, for some integer k . Let b have remainder r when divided by n , so that $b = nq + r$ for some integer q . Then

$$a = b + kn = nq + r + kn = (q + k)n + r$$

shows that a has the same remainder, r , as b . ■

1.2 Residue classes

One outcome of Proposition 1.4 is that every integer is congruent to exactly one of the integers $0, 1, 2, \dots, n - 1$ modulo n , namely whichever one of these is its remainder on dividing by n . This set of n integers is called the set of **least positive residues** modulo n . (Strictly speaking, since 0 is not a positive integer, it ought to be called the set of *least non-negative residues*, but this misnomer is firmly entrenched in the literature.)

Furthermore, we can split up $\mathbb{Z}$ into non-overlapping sets called **residue** (or **congruence**) **classes**, where two integers belong to the same class if, and only if, they are congruent modulo n . For example, for the case $n = 4$ the residue classes are as follows.

$$\begin{aligned} &\{\dots, -8, -4, 0, 4, 8, \dots\} \\ &\{\dots, -7, -3, 1, 5, 9, \dots\} \\ &\{\dots, -6, -2, 2, 6, 10, \dots\} \\ &\{\dots, -5, -1, 3, 7, 11, \dots\} \end{aligned}$$

A set obtained by selecting one member from each of these residue classes, for example $\{0, 1, 2, 3\}$ or $\{8, -3, 22, -9\}$, is called a **complete set of residues** modulo 4. In general, a set $\{a_1, a_2, a_3, \dots, a_n\}$ of n integers is a complete set of residues modulo n provided no two of them are congruent modulo n . By virtue of Proposition 1.4 this will mean that the integers $\{a_1, a_2, a_3, \dots, a_n\}$ are congruent, in some order, to $\{0, 1, 2, \dots, n - 1\}$ modulo n .

In choosing a complete set of residues modulo n , our most frequent selection will be the set of least positive residues, $\{0, 1, 2, \dots, n - 1\}$. However, we will have occasion to use the set of **least absolute residues** obtained by choosing, from each residue class, the one with least modulus. To be precise, from each residue class modulo n we choose the unique member x that lies in the range $-\frac{1}{2}n < x \leq \frac{1}{2}n$. For example, the set of least absolute residues for $n = 4$ is $\{-1, 0, 1, 2\}$ whilst for $n = 7$ it is $\{-3, -2, -1, 0, 1, 2, 3\}$.

Exercise 1.3

- (a) Write down the set of least positive residues modulo n , and the set of least absolute residues modulo n , for (i) $n = 10$ and (ii) $n = 11$.
- (b) Determine whether or not each of the following sets is a complete set of residues modulo 11.
- (i) $\{6, 2, -3, 22, 23, -7, 7, 9, 43, -8, 16\}$
 - (ii) $\{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2\}$
 - (iii) $\{0, 1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$

Properties (d) and (e) of Theorem 1.2 are of great importance. In essence they say that the residue class to which a sum $a + c$, or a product ac , belongs does not depend on the individual numbers a and c , but rather on the residue classes to which they belong. To clarify this remark, let us denote by $[r]$ the residue class modulo n to which the integer r belongs. So

$$[r] = \{\dots, r - 2n, r - n, r, r + n, r + 2n, \dots\}.$$

This will mean that residue classes are denoted in many different ways; for example when $n = 5$, $[-1] = [4] = [19]$ since $-1 \equiv 4 \equiv 19 \pmod{5}$. In this notation, properties (d) and (e) can be restated as follows.

(d) If $[a] = [b]$ and $[c] = [d]$ then $[a + c] = [b + d]$.

(e) If $[a] = [b]$ and $[c] = [d]$ then $[ac] = [bd]$.

These two facts amount to saying that the operations defined by

$$[a] + [c] = [a + c] \text{ and } [a] \times [c] = [ac]$$

on the set of residue classes modulo n are unambiguous. Whatever numbers are chosen to represent the two residue classes, the sum of the numbers will always belong to the same class, as will the product of the numbers.

Let

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

be the set of all residue classes modulo n . Together with the operations of addition and multiplication defined above, we have an arithmetic on $\mathbb{Z}_n$.

For example, taking $n = 4$ we have the tables

+	[0]	[1]	[2]	[3]	×	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[0]	[1]	[0]	[1]	[2]	[3]
[2]	[2]	[3]	[0]	[1]	[2]	[0]	[2]	[0]	[2]
[3]	[3]	[0]	[1]	[2]	[3]	[0]	[3]	[2]	[1]

where, for example, $[3] \times [2] = [2]$ is obtained from the definition

$$[3] \times [2] = [3 \times 2] = [6]$$

and the fact that $[6] = [2]$ since $6 \equiv 2 \pmod{4}$.

Exercise 1.4

Working in $\mathbb{Z}_{10}$, determine $[6] + [8]$ and $[6] \times [8]$ and find all $[b]$ such that $[6] \times [b] = [8]$.

Repeat the above, this time working in $\mathbb{Z}_{11}$.

A problem in congruence modulo n is equivalent to a problem in $\mathbb{Z}_n$ with its arithmetic as illustrated in Exercise 1.4 above. In practice, however, we abandon much of this formalism. What we will do is select a complete set of residues (usually the set of least positive residues) and work with these numbers, dropping the square brackets. When any sum or product is calculated we replace the answer with the chosen residue to which it is congruent. Here are a couple of illustrations of the way in which congruence is used.

Worked Exercise 1.5

- (a) Show that $1^3 + 2^3 + 3^3 + \cdots + 60^3$ is divisible by 5.
- (b) Show that there do not exist integers x and y such that $x^2 + y^2 = 999$.

Solution

- (a) In terms of congruence we are asked to show that $1^3 + 2^3 + 3^3 + \cdots + 60^3$ is congruent to 0 modulo 5. Now each of the terms r^3 is congruent to one of 0, 1, 2, 3 or 4 modulo 5, and so one line of attack would be to evaluate the least positive residue modulo 5 of each of these cubes and add up. However, a considerable shortcut is provided by Theorem 1.2(f), which tells us that if two numbers are congruent modulo 5 then their cubes are also congruent modulo 5. So, since $1 \equiv 6 \equiv 11 \equiv \cdots \equiv 56 \pmod{5}$, we have

$$1^3 \equiv 6^3 \equiv 11^3 \equiv \cdots \equiv 56^3 \pmod{5}.$$

Similarly

$$2^3 \equiv 7^3 \equiv 12^3 \equiv \cdots \equiv 57^3 \pmod{5},$$

$$3^3 \equiv 8^3 \equiv 13^3 \equiv \cdots \equiv 58^3 \pmod{5},$$

$$4^3 \equiv 9^3 \equiv 14^3 \equiv \cdots \equiv 59^3 \pmod{5},$$

$$5^3 \equiv 10^3 \equiv 15^3 \equiv \cdots \equiv 60^3 \pmod{5}.$$

Therefore,

$$1^3 + 2^3 + 3^3 + \cdots + 60^3 \\ \equiv 12 \times (1^3 + 2^3 + 3^3 + 4^3 + 5^3) \pmod{5}.$$

Now,

$$2^3 = 8 \equiv 3, \quad 3^3 = 27 \equiv 2, \quad 4^3 = 64 \equiv 4 \\ \text{and } 5^3 \equiv 0^3 \equiv 0 \pmod{5},$$

and so

$$1^3 + 2^3 + 3^3 + \cdots + 60^3 \equiv 12 \times (1 + 3 + 2 + 4 + 0) = 120 \\ \equiv 0 \pmod{5},$$

as claimed.

- (b) At first glance it might be difficult to see what this question has to do with congruence. In fact, it is a particular case of a general result concerning the possible values that a sum of two squares can take modulo 4.

Any integer x is congruent to one of the integers 0, 1, 2 or 3 modulo 4. Theorem 1.2(f) tells us that x^2 is therefore congruent to one of the numbers 0^2 , 1^2 , 2^2 or 3^2 modulo 4. That is, x^2 is congruent to either 0 or 1 modulo 4 (since $2^2 \equiv 0 \pmod{4}$ and $3^2 \equiv 1 \pmod{4}$). Similarly, for any integer y , y^2 is congruent to either 0 or 1 modulo 4. Theorem 1.2(d) now gives

$$x^2 + y^2 \equiv 0, 1 \text{ or } 2 \pmod{4}$$

(as 0, 1 and 2 are the possible results of adding either 0 or 1 to either 0 or 1).

This argument tells us that any integer that is congruent to 3 modulo 4 cannot be written as the sum of two squares. Now $999 \equiv 3 \pmod{4}$ is such an integer, and so the equation

$$x^2 + y^2 = 999$$

cannot have a solution in integers.

There are simpler ways of solving Worked Exercise 1.5(a).

For instance, you may be familiar with the formula

$$\sum_{r=1}^n r^3 = \left(\frac{n(n+1)}{2} \right)^2,$$

in which case you could deduce the result by putting $n = 60$.

Our solution here intentionally illustrates the use of the properties of congruence.

And now some problems for you to solve.

Exercise 1.5

- (a) What is the remainder when $1! + 2! + 3! + \cdots + 1000!$ is divided by 7?
 (b) Let a be an integer that is not divisible by either 2 or 3. Prove that $a^2 - 1$ is divisible by 24.

Hint: show $a^2 \equiv 1 \pmod{24}$.

1.3 Further properties

There is a property of congruence that, although it is no more than a re-expression of an established divisibility property, will be used so often that it merits the status of a theorem.

Theorem 1.6

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, then
 $a \equiv b \pmod{\text{lcm}(m, n)}$.

Proof From the definition of congruence there exist integers r and s such that

$$a - b = rm \quad \text{and} \quad a - b = sn.$$

Let $d = \text{hcf}(m, n)$, so that

$$m = dm' \quad \text{and} \quad n = dn', \quad \text{where } \text{hcf}(m', n') = 1.$$

Substituting for m and n in the equation $rm = sn$ gives

$$rdm' = sdn'; \text{ that is, } rm' = sn'.$$

We infer from this that n' divides rm' , whereupon Euclid's Lemma gives us that n' divides r . So putting $r = kn'$ we have

$$a - b = rm = kmn' = km \left(\frac{n}{d} \right) = k \left(\frac{mn}{d} \right) = k \text{lcm}(m, n).$$

That is, $a \equiv b \pmod{\text{lcm}(m, n)}$, as claimed. ■

One particular case of Theorem 1.6 is well worth highlighting. We will frequently want to apply this result when m and n are coprime, in which case $\text{lcm}(m, n) = mn$.

Corollary 1.7 to Theorem 1.6

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $\text{hcf}(m, n) = 1$, then
 $a \equiv b \pmod{mn}$.

Notice how much simpler Exercise 1.5(b) would have been with the benefit of Theorem 1.6. To show that $a^2 \equiv 1 \pmod{24}$ it is sufficient to show that $a^2 \equiv 1 \pmod{8}$ and $a^2 \equiv 1 \pmod{3}$. Both these separate parts are quickly confirmed from congruence ideas:

(1) a odd implies $a \equiv 1, 3, 5$ or $7 \pmod{8}$, and squaring,

$$a^2 \equiv 1 \pmod{8} \text{ in all cases;}$$

(2) a not divisible by 3 implies $a \equiv 1$ or $2 \pmod{3}$, and squaring,

$$a^2 \equiv 1 \pmod{3} \text{ in each case.}$$

We have seen that if $a \equiv b \pmod{n}$ then $ca \equiv cb \pmod{n}$, for any integer c . What about the converse of this result? If $ca \equiv cb \pmod{n}$ can we

Proposition 4.10 of Chapter 1 establishes that $\text{hcf}(m', n') = 1$.

See Proposition 4.15 of Chapter 1.

legitimately cancel the cs to recover $a \equiv b \pmod{n}$? In fact we cannot, as this simple counter-example shows:

$$2 \equiv 8 \pmod{6} \text{ but } 1 \not\equiv 4 \pmod{6}.$$

Here, cancellation of the common factor 2 has produced a contradiction.

Common factors on two sides of a congruence can always be cancelled, but in doing so the modulus has to be adjusted according to the following rule.

Proposition 1.8 Cancellation Rule

If $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{\frac{n}{d}}$, where $d = \text{hcf}(c, n)$.

Proof From $ca \equiv cb \pmod{n}$ we know that there exists an integer k such that $ca - cb = kn$. Now $\text{hcf}(c, n) = d$, and so there exist coprime integers r and s such that $c = dr$ and $n = ds$. Therefore, substituting for c and n in the equation $ca - cb = kn$ gives

$$dra - drb = kds,$$

which, after cancelling the common d , gives

$$r(a - b) = ks.$$

From this s divides $r(a - b)$ and, as $\text{hcf}(r, s) = 1$, Euclid's Lemma confirms that s divides $a - b$. Consequently $a \equiv b \pmod{s}$, where $s = \frac{n}{d}$. ■

Proposition 4.10 of Chapter 1 established that r and s are coprime.

Let us revisit the counter-example from before the proposition. Given $2 \equiv 8 \pmod{6}$, we see that $\text{hcf}(2, 6) = 2$, so we can cancel the 2 by also dividing the modulus by 2. Thus $1 \equiv 4 \pmod{3}$.

One special case of Proposition 1.8 is worth noting: when $\text{hcf}(c, n) = 1$ the common factor c can be cancelled without the need to adjust the modulus. This is stated formally as follows.

Corollary 1.9 to the Cancellation Rule

If $ca \equiv cb \pmod{n}$, where $\text{hcf}(c, n) = 1$, then $a \equiv b \pmod{n}$.

In fact, the two congruences in Proposition 1.8 are 'equivalent' because the reverse implication also holds. That is,

$$\text{if } a \equiv b \pmod{\frac{n}{d}} \text{ then } ca \equiv cb \pmod{n}, \text{ where } d = \text{hcf}(c, n).$$

To justify this remark, suppose that $a \equiv b \pmod{\frac{n}{d}}$. Then there is an integer k such that

$$a - b = k\frac{n}{d}.$$

Multiplying by c gives

$$ca - cb = \frac{kc}{d}n,$$

so that $ca \equiv cb \pmod{n}$, since $\frac{c}{d}$ is an integer.

For example, the congruence $12x \equiv 18 \pmod{27}$ can be simplified by cancellation of the common factor 6 and dividing the modulus by $\text{hcf}(6, 27) = 3$. So if $12x \equiv 18 \pmod{27}$ then $2x \equiv 3 \pmod{9}$ by the Cancellation Rule.

Conversely, if $2x \equiv 3 \pmod{9}$ then, as argued above, we also have $12x \equiv 18 \pmod{27}$. We make use of the symbol $\iff$ (pronounced in this context as ‘is equivalent to’) to indicate that two congruences are ‘equivalent’. Thus we can write

$$12x \equiv 18 \pmod{27} \iff 2x \equiv 3 \pmod{9}.$$

The congruences are **equivalent** in the sense that an integer x is a solution of one congruence if, and only if, it is a solution of the other.

Exercise 1.6

Use an appropriate cancellation to simplify each of the following congruences:

- (a) $6x \equiv 18 \pmod{30}$
- (b) $20x \equiv 30 \pmod{45}$
- (c) $52x \equiv 39 \pmod{60}$.

Before we leave this area of congruence properties there is one final result that merits our attention. Euclid’s Lemma for the case of a prime factor p showed that if p divides ab , then either p divides a or p divides b . When this is expressed in congruence notation we have the result that follows. We will have numerous occasions to refer to this result so, to ease identification of the reference, we will continue to call it Euclid’s Lemma for prime factors.

Theorem 1.10 *Euclid’s Lemma for prime factors*

If $ab \equiv 0 \pmod{p}$ then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Exercise 1.7

- (a) Determine the least positive residue and the least absolute residue of 1997:
- (i) modulo 7
 - (ii) modulo 17
 - (iii) modulo 101.
- (b) Suppose that $k \equiv 1 \pmod{12}$ for some integer k . What is the least positive residue of $6k + 5$:
- (i) modulo 4
 - (ii) modulo 9
 - (iii) modulo 12?
- (c) (i) Give an example to show that $a^k \equiv b^k \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.
- (ii) Give an example to show that $a^k \equiv b^k \pmod{n}$ and $k \equiv j \pmod{n}$ both being true does not necessarily imply that $a^j \equiv b^j \pmod{n}$ is true.
- (d) Prove by induction that $6^n \equiv 5n + 1 \pmod{25}$, for all integers $n \geq 1$.
- (e) Prove that if $n \geq 2$ and $\text{hcf}(a, n) = 1$ then the set of integers
- $$\{c, c + a, c + 2a, c + 3a, \dots, c + (n - 1)a\}$$
- is a complete set of residues modulo n for any integer c .
- (f) What is the remainder when 11^{11} is divided by:
- (i) 7
 - (ii) 17
 - (iii) 19?
- (g) Use ideas of congruence to prove that:
- (i) 29 divides $2^{28} - 1$
 - (ii) 79 divides $3^{39} + 1$.
- (h) In 1659 Fermat asserted that no prime number of the form $3k - 1$ can be written in the form $a^2 + 3b^2$. Use congruence modulo 3 to show that he was correct.
- (i) From the definition of congruence alone, prove the following.
If $ar \equiv b \pmod{n}$ and $cr \equiv d \pmod{n}$, for some integer r , then $ad \equiv bc \pmod{n}$.

In Exercise 1.3 we have made a start at solving congruence problems. We will return to this in Section 3, but first, in Section 2, we take a short detour.

2 Divisibility tests

Given any integer written in our familiar decimal representation, we can tell at a glance whether or not it is divisible by 2 or 5. To test divisibility by 5, for example, we simply look to see whether or not the units digit is 0 or 5. Though not quite so immediate, there are also fairly simple tests for divisibility by 3, 4, 8, 9 and 11. All these divisibility tests can be derived from congruence ideas.

Historically, the most significant divisibility test is that for division by 9.

A natural number is divisible by 9 if, and only if, the sum of its digits is divisible by 9.

In fact this is a special case of a stronger result, which we will prove shortly.

A natural number is congruent to the sum of its digits modulo 9.

For example, if $N = 974064$ then

$$N \equiv 9 + 7 + 4 + 0 + 6 + 4 = 30 \equiv 3 \pmod{9}.$$

This fact led to a method of checking calculations, known as ‘casting out nines’, which, over the years, has been much used by bookkeepers. The method amounts to reworking the calculations in the residue class arithmetic $\mathbb{Z}_9$. As an illustration, consider the multiplication shown in Figure 2.1. On the left the multiplication is carried out fully, whilst on the right the same calculation is carried out modulo 9.

$ \begin{array}{r} 1489 \\ \times 753 \\ \hline 1042300 \\ 74450 \\ 4467 \\ \hline 1121217 \end{array} $	$ \begin{aligned} 1 + 4 + 8 + 9 &= 22 \equiv 4 \pmod{9} \\ 7 + 5 + 3 &= 15 \equiv 6 \pmod{9} \\ 4 \times 6 &= 24 \equiv 6 \pmod{9} \\ \text{Check: } 1 + 1 + 2 + 1 + 2 + 1 + 7 &= 15 \equiv 6 \pmod{9} \end{aligned} $
---	---

Figure 2.1 Casting out nines

The fact that the two answers agree modulo 9 is far from being conclusive proof that the calculation is correct. However, there is a good chance that a mistake in carrying out the calculation would have shown up during this check.

In the following proposition we prove the results that give divisibility tests for 9 and 11 together.

Proposition 2.1 *Divisibility by 9 and 11*

Let the integer N be written in decimal notation as $N = a_m a_{m-1} \dots a_2 a_1 a_0$ so that the digits satisfy $0 \leq a_i \leq 9$ with $a_m \neq 0$. Then:

- (a) $N \equiv a_0 + a_1 + a_2 + a_3 + \dots + a_m \pmod{9}$
- (b) $N \equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m \pmod{11}$.

Proof The key is to write out the number N in terms of powers of 10, namely

$$N = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + \dots + 10^m a_m.$$

- (a) Since $10 \equiv 1 \pmod{9}$, it follows from Theorem 1.2(f) that $10^r \equiv 1 \pmod{9}$ for all integers $r \geq 1$. Thus, from properties (d) and (e) of Theorem 1.2,

$$\begin{aligned} N &\equiv a_0 + 1a_1 + 1a_2 + 1a_3 + \dots + 1a_m \pmod{9} \\ &\equiv a_0 + a_1 + a_2 + a_3 + \dots + a_m \pmod{9}. \end{aligned}$$

- (b) Similarly, since $10 \equiv -1 \pmod{11}$, $10^r \equiv (-1)^r \pmod{11}$ for all integers r and

$$\begin{aligned} N &\equiv a_0 + (-1)a_1 + (-1)^2a_2 + \dots + (-1)^m a_m \pmod{11} \\ &\equiv a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m \pmod{11}. \quad \blacksquare \end{aligned}$$

In the congruences of parts (a) and (b) of Proposition 2.1, and in their proofs, we have unnecessarily used the digits of N in reverse order, starting at the units digit a_0 . It will be helpful to use formula (b) in this way, starting at the positive units digit and then alternating the signs. But in using formula (a) we will often, as we did in Figure 2.1 above, add the digits in their naturally occurring order.

The two special cases in which $N \equiv 0$ in parts (a) and (b) of Proposition 2.1 can be restated as the following result.

Corollary 2.2 *to Proposition 2.1*

- (a) A natural number N is divisible by 9 if, and only if, the sum of its digits is divisible by 9.
- (b) A natural number N is divisible by 11 if, and only if, the alternating sum of its digits is divisible by 11, where by ‘alternating sum’ we mean the sum using alternating signs as given in part (b) of Proposition 2.1.

The following well-known test for division by 3 follows from part (a) of Proposition 2.1.

Proposition 2.3

A natural number N is divisible by 3 if, and only if, the sum of its digits is divisible by 3.

Proof First we show that if N is divisible by 3, then the sum of its digits is divisible by 3. Let N be divisible by 3, that is, $N = 3s$, for some natural number s . Substituting $3s$ for N in Proposition 2.1(a) gives $3s \equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_m \pmod{9}$, which, by the definition of congruence, means that there is an integer t such that

$$a_0 + a_1 + a_2 + a_3 + \cdots + a_m - 3s = 9t.$$

It follows that

$$a_0 + a_1 + a_2 + a_3 + \cdots + a_m = 3s + 9t = 3(s + 3t),$$

which shows that the digit sum is divisible by 3.

Conversely, suppose that the digit sum of N is divisible by 3, that is, the digit sum is equal to $3s$ for some natural number s . Substituting $3s$ for the digit sum in the congruence of Proposition 2.1(a) now gives $N \equiv 3s \pmod{9}$. It follows that $N - 3s = 9t$ for some integer t . Hence

$$N = 3s + 9t = 3(s + 3t),$$

which shows that N is divisible by 3. ■

Exercise 2.1

- (a) Let $N = 9723$ and $M = 18\,056$.
- (i) Determine the remainders when each of the numbers N , M , $N + M$ and $N - M$ is divided by 9.
 - (ii) Determine the remainders when each of the numbers N , M , $N + M$ and $N - M$ is divided by 11.
 - (iii) Determine the missing digit (?) in the product

$$N \times M = 9723 \times 18\,056 = 175(?)58\,488$$

without using a calculator.

- (b) An integer N has an even number of digits. A second integer M is formed by moving the last digit of N to the front. (For example, if $N = 588\,471$ then the 1 is moved to the front, giving $M = 158\,847$.) Show that 9 divides $N - M$, 11 divides $N + M$ and 99 divides $N^2 - M^2$.

There are numerous variations on the following trick, which capitalises on the connection between a number and the sum of its digits. A person is asked to think of any 3-digit number (that is not palindromic). Without knowing what the number is, a prediction is made that application of the

following sequence of operations on the number will produce the answer 1089.

Write down the number and the number formed by reversing the order of its digits. Then subtract the smaller of these numbers from the larger. Finally add to this the number formed by reversing its digits.

For example, if the chosen number is 638 then this is subtracted from 836, giving 198. Adding 198 to 891 gives 1089. The work of this section should enable you to explain why this is so: using an argument similar to that in part (b) of the above exercise should allow you to deduce that the subtraction always gives a number that is divisible by 99. This fact restricts the values that the three digits of this number can take and the result follows.

It may happen that the first subtraction produces a 2-digit number. This is treated as a 3-digit number with leading 0 for the purposes of reversing its digits. For example, 99 would reverse to 990.

Exercise 2.2

- (a) Without carrying out the multiplication, find the missing digit (?) in each of the following products.
- (i) $108 \times 371 = 400(?)8$
 - (ii) $1578 \times 34971 = 5518(?)238$
 - (iii) $4473 \times 3(?)9 = 1426887$
- Hint:* for part (iii), test for divisibility by 11.
- (b) A and B are two different 7-digit numbers, each involving all seven of the digits 1, 2, 3, 4, 5, 6 and 7. Prove that A does not divide B .
- (c) Let $N > M$ be two 10-digit numbers formed from the same 10 digits but in different orders. If X is the sum of the digits of $N - M$, show that the sum of the digits of X is 9.
- (d) Show that 2^n divides an integer N if, and only if, 2^n divides the number made up of the last n digits of N .
- (e) (i) Show that, for all $n \geq 0$, $10^{2n} \equiv 1 \pmod{99}$ and $10^{2n+1} \equiv 10 \pmod{99}$.

- (ii) The remainder on dividing a number by 99 can be found in a way similar to the corresponding result for division by 9, but treating the digits of the number two at a time. The following examples illustrate the method:

$$6239 \equiv 62 + 39 = 101 \equiv 2 \pmod{99}$$

and

$$54787 \equiv 5 + 47 + 87 = 139 \equiv 40 \pmod{99}.$$

Use the result in part (i) to show why this test works.

- (iii) Find a test for divisibility by 101 and use it to determine the remainders when 62479 and 9850833 are divided by 101.

3 Linear congruences

Having studied basic properties of congruence, the next step is to look at the problem of solving congruences involving unknowns, such as $3x \equiv 7 \pmod{12}$ or $x^5 - x^3 \equiv 0 \pmod{8}$. The first of these examples happens to have no solutions, for there is no integer x for which $3x \equiv 7 \pmod{12}$. On the other hand, every integer x satisfies $x^5 - x^3 \equiv 0 \pmod{8}$ – try one!

3.1 Polynomial congruences

By an **integral polynomial** we mean a polynomial

$$P(x) = c_mx^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$$

in which the coefficients $c_0, c_1, \dots, c_m$ and the variable x are integers. If $P(x)$ is an integral polynomial then the congruence $P(x) \equiv 0 \pmod{n}$ is a **polynomial congruence**. Our present interest is in solving polynomial congruences and we show straight away that if an integer a is a solution of the congruence, that is, $P(a) \equiv 0 \pmod{n}$, then so too is every integer in the residue class of a modulo n .

Proposition 3.1

Let $P(x)$ be an integral polynomial. If $a \equiv b \pmod{n}$ then $P(a) \equiv P(b) \pmod{n}$. In particular, a is a solution of the polynomial congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, b is a solution.

Proof Let $P(x) = c_mx^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$. Since $a \equiv b \pmod{n}$, properties (e) and (f) of Theorem 1.2 of this chapter tell us that $c_ra^r \equiv c_rb^r \pmod{n}$, for each integer $r \geq 1$. Property (d) of Theorem 1.2 then gives

$$\begin{aligned} P(a) &= c_ma^m + c_{m-1}a^{m-1} + \cdots + c_1a + c_0 \\ &\equiv c_mb^m + c_{m-1}b^{m-1} + \cdots + c_1b + c_0 \equiv P(b) \pmod{n}. \end{aligned}$$

In particular, $P(a) \equiv 0 \pmod{n}$ if, and only if, $P(b) \equiv 0 \pmod{n}$. That is, a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if, and only if, b is a solution. ■

As a consequence of Proposition 3.1, it is apparent that the problem of solving the congruence $P(x) \equiv 0 \pmod{n}$ is really a problem in the residue class arithmetic $\mathbb{Z}_n$; if an integer is a solution then so too is every integer in its residue class. So the task is to find which residue classes solve the congruence. Two congruent integers that satisfy a polynomial congruence will be thought of as being the *same* solution.

Definition 3.2 *Number of solutions of a polynomial congruence*

Let $S = \{b_1, b_2, \dots, b_n\}$ be a complete set of residues modulo n . The *number of solutions* of the congruence $P(x) \equiv 0 \pmod{n}$ is the number of integers $b \in S$ for which $P(b) \equiv 0 \pmod{n}$.

Here is an example.

Worked Exercise 3.3

Solve the polynomial congruence $x^2 - x \equiv 0 \pmod{6}$.

Solution

There are six residue classes modulo 6 and each may be a solution of the congruence. We choose the least positive residues, 0, 1, 2, 3, 4 and 5, and test each one in turn.

$$0^2 - 0 \equiv 0 \pmod{6}$$

$$1^2 - 1 \equiv 0 \pmod{6}$$

$$2^2 - 2 \equiv 2 \pmod{6}$$

$$3^2 - 3 \equiv 0 \pmod{6}$$

$$4^2 - 4 \equiv 0 \pmod{6}$$

$$5^2 - 5 \equiv 2 \pmod{6}$$

We see that 0, 1, 3 and 4 are solutions of the congruence and therefore so too is any integer congruent to one of 0, 1, 3 or 4 modulo 6. On the other hand, any integer that is congruent to either 2 or 5 modulo 6 does not satisfy the congruence. The congruence has *four* solutions:

$$x \equiv 0, 1, 3, 4 \pmod{6}.$$

Exercise 3.1

Solve the following polynomial congruences.

(a) $P_1(x) = x^2 + 3x + 4 \equiv 0 \pmod{7}$

(b) $P_2(x) = x^4 - 1 \equiv 0 \pmod{5}$

This method of solving a problem by checking every possible candidate is called **solution by exhaustion**.

3.2 Linear congruences

We have quickly found an algorithmic method for solving polynomial congruences – namely, substitute for x , in turn, each value from any complete set of residues and record the resulting zeros. This is all well and good when the modulus in question is reasonably small and the degree of the polynomial is not too large. For more awkward polynomials the amount of computation involved in this sledgehammer attack quickly renders it impractical, and we must look around for something more subtle. In Chapter 4 we return to the problem of solving general polynomial congruences. There you will discover ways of simplifying polynomial congruences and will learn to predict how many solutions a given polynomial congruence has. Book C, Chapter 10 is concerned with quadratic congruences and their solutions. For the remainder of this chapter we confine our attention to the linear congruence

$$ax \equiv b \pmod{n}.$$

This, the simplest of all polynomial congruences, crops up naturally in a variety of situations in number theory.

Suppose that x_0 is an integer such that $ax_0 \equiv b \pmod{n}$. This means that n divides $ax_0 - b$ or, put another way, there exists an integer y_0 such that

$$ax_0 - b = ny_0.$$

Rearranging this equation tells us that $x = x_0, y = y_0$ is a solution of the linear Diophantine equation $ax - ny = b$. On the other hand if $x = x_0, y = y_0$ is any solution of $ax - ny = b$ then it is certainly the case that $ax_0 \equiv b \pmod{n}$. Thus the problem of finding all integers satisfying the linear congruence $ax \equiv b \pmod{n}$ is precisely the same problem as finding all x -values in solutions of the linear Diophantine equation $ax - ny = b$. As we have already solved the latter problem in Theorem 5.4 of Chapter 1, our principal result on linear congruences is little more than a re-expression of that earlier theorem.

Theorem 3.4 *Solution of linear congruences*

Consider the linear congruence $ax \equiv b \pmod{n}$.

- (a) The congruence has solutions if, and only if, $\text{hcf}(a, n)$ divides b .
- (b) If $\text{hcf}(a, n) = 1$, the congruence has a unique solution.
- (c) If $\text{hcf}(a, n) = d$ and d divides b , then the congruence has d solutions, which are given by the unique solution modulo $\frac{n}{d}$ of the congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Proof

- (a) The linear Diophantine equation $ax - ny = b$ has solutions if, and only if, $\text{hcf}(a, n)$ divides b . From the remarks preceding the theorem, it follows that the congruence $ax \equiv b \pmod{n}$ has solutions if, and only if, $\text{hcf}(a, n)$ divides b .
- (b) Suppose that $\text{hcf}(a, n) = 1$. Theorem 5.4 of Chapter 1 tells us that if $x = x_0, y = y_0$ is one solution of $ax - ny = b$, then the general solution is

$$x = x_0 + nk, \quad y = y_0 + ak, \quad k \in \mathbb{Z}.$$

But for all integers k

$$x_0 + nk \equiv x_0 \pmod{n}$$

and so $x \equiv x_0 \pmod{n}$ is the only solution of $ax \equiv b \pmod{n}$.

- (c) If $\text{hcf}(a, n) = d$ and d divides b then

$$ax \equiv b \pmod{n} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

But $\text{hcf}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, and so the right-hand congruence has a unique solution modulo $\frac{n}{d}$, say

$$x \equiv x_1 \pmod{\frac{n}{d}}.$$

Hence the integers x that satisfy $ax \equiv b \pmod{n}$ are precisely those of the form $x = x_1 + k\frac{n}{d}$, for some integer k .

Consider the set of d integers

$$\left\{x_1, x_1 + \frac{n}{d}, x_1 + 2\frac{n}{d}, \dots, x_1 + (d-1)\frac{n}{d}\right\}.$$

Certainly no two of these integers are congruent modulo n , because they are distinct and no two differ by as much as n . We claim further that, for any integer k , $x_1 + k\frac{n}{d}$ is congruent to one of them modulo n . To see why that is so, write $k = dq + r$, where $0 \leq r < d$, as given by the Division Algorithm. Then

$$\begin{aligned} x_1 + k\frac{n}{d} &= x_1 + (dq + r)\frac{n}{d} = x_1 + nq + r\frac{n}{d} \\ &\equiv x_1 + r\frac{n}{d} \pmod{n}. \end{aligned}$$

So these are the d solutions of $ax \equiv b \pmod{n}$. ■

To illustrate part (c) and its proof, consider the congruence

$$12x \equiv 15 \pmod{21}.$$

Since $\text{hcf}(12, 21) = 3$, and 3 divides 15, the congruence has three solutions modulo 21.

Cancellation of the common 3 reduces the congruence to

$$4x \equiv 5 \pmod{7}$$

which has a unique solution modulo 7, since $\text{hcf}(4, 7) = 1$. That solution is

$$x \equiv 3 \pmod{7}$$

as can be seen from $4 \times 3 \equiv 5 \pmod{7}$. The argument in the proof of part (c) then supplies the three solutions modulo 21 as

$$\begin{aligned}x &\equiv 3 \pmod{21}, \\x &\equiv 3 + 7 = 10 \pmod{21} \text{ and} \\x &\equiv 3 + 2 \times 7 = 17 \pmod{21}.\end{aligned}$$

Exercise 3.2

How many solutions does each of the following linear congruences have?

- (a) $5x \equiv 13 \pmod{10}$
- (b) $5x \equiv 10 \pmod{13}$
- (c) $10x \equiv 5 \pmod{30}$
- (d) $27x \equiv 318 \pmod{24}$

3.3 Solving linear congruences

It is nice to have a theoretical result telling us that solutions exist, but it is more important to be able to find those solutions.

Worked Exercise 3.5

Solve the linear congruence $30x \equiv 15 \pmod{33}$.

Solution

As $\text{hcf}(30, 33) = 3$ and 3 divides 15, Theorem 3.4 guarantees that the congruence has three solutions modulo 33. Failing all else, we know that we could find these solutions by substituting for x each of the values $0, 1, 2, 3, \dots, 32$ and recording which are solutions. But this last resort can usually be avoided, and can here, as we will illustrate.

For a start we can use the cancellation laws to reduce the modulus. By the Cancellation Rule, Proposition 1.8 of this chapter, the common factor 3 in both coefficients and modulus can be cancelled to give the equivalent congruence

$$10x \equiv 5 \pmod{11}.$$

As $\text{hcf}(10, 11) = 1$ we know, by Theorem 3.4(b), that this congruence has a unique solution modulo 11.

Next we can cancel further. By the Cancellation Rule the common factor 5 in the coefficients can be cancelled, this time the modulus remaining unchanged:

$$2x \equiv 1 \pmod{11}.$$

There are a number of ways of determining the unique solution modulo 11 from here. For example, we could replace the number 1 on the right-hand side of the congruence with 12, since $1 \equiv 12 \pmod{11}$:

$$2x \equiv 12 \pmod{11}.$$

Finally, cancellation of the common factor 2 of the coefficients yields the solution:

$$x \equiv 6 \pmod{11}.$$

Alternatively we could have multiplied through the congruence $2x \equiv 1 \pmod{11}$ by 6, obtaining

$$12x \equiv 6 \pmod{11},$$

whereupon replacement of the coefficient 12 by the congruent number 1 yields the same solution

$$x \equiv 6 \pmod{11}.$$

We noted that the original congruence had three solutions modulo 33 and we have ended with a unique solution modulo 11. There is no contradiction to Theorem 3.4 here, for in the set of least positive residues modulo 33 there are three numbers, namely 6, 17 and 28, that are congruent to 6 modulo 11. Consequently the unique solution $x \equiv 6 \pmod{11}$ is equivalent to the three solutions

$$x \equiv 6, 17, 28 \pmod{33},$$

for both determine the same set of integers, namely,

$$\{\dots, -38, -27, -16, -5, 6, 17, 28, 39, 50, \dots\}.$$

So either form can be taken as the answer here. Normally, except when the context of the problem demands otherwise, we will always give the solution(s) in terms of the original modulus.

Linear congruences, like the one we have just tackled, can all be solved using the following strategy.

Strategy: to solve the linear congruence $ax \equiv b \pmod{n}$

1. Check that $\text{hcf}(a, n)$ divides b . If it does not, the congruence has no solutions. If it does:
2. Cancel any common factors of all three of a , b and n . The resulting congruence has a unique solution modulo the new modulus.

The resulting coefficients (originally a and b) can then be changed by applying the remaining steps in any order, any number of times, with the goal of reaching a congruence in which the coefficient of x is 1.

3. Cancel any common factor of the coefficients.
4. Replace either coefficient by any congruent number.
5. Multiply through the congruence by any number that is coprime to the modulus.

Step 5 needs a little clarification. To illustrate why the multiplier has to be coprime to the modulus, consider the congruence

$$7x \equiv 1 \pmod{40}.$$

If we multiply through by 6 we get

$$42x \equiv 6 \pmod{40},$$

and replacing 42 with the congruent number 2 gives

$$2x \equiv 6 \pmod{40}.$$

Plainly $x \equiv 3 \pmod{40}$ is a solution of this congruence because $2 \times 3 \equiv 6 \pmod{40}$, but it is not a solution of the original congruence because $7 \times 3 = 21 \not\equiv 1 \pmod{40}$. So somewhere along the line an extraneous solution has been introduced.

The problem arose when we multiplied through the congruence by 6, because $\text{hcf}(6, 40) > 1$. From $ax \equiv b \pmod{n}$ it is certainly true that $cax \equiv cb \pmod{n}$. But, according to Proposition 1.8, the Cancellation Rule, we can reverse the argument and draw the conclusion $ax \equiv b \pmod{n}$ from $cax \equiv cb \pmod{n}$ only when $\text{hcf}(c, n) = 1$. A solution of $cax \equiv cb \pmod{n}$ is not necessarily a solution of $ax \equiv b \pmod{n}$ unless $\text{hcf}(c, n) = 1$. Hence the coprime condition of step 5 must hold before we multiply through a congruence.

The way to become proficient at solving linear congruences is through plenty of practice at applying the above strategy. We do one more before inviting you to try your hand.

Worked Exercise 3.6

Solve $9x \equiv 15 \pmod{26}$.

Solution

As $\text{hcf}(9, 26) = 1$, step 1 tells us that $9x \equiv 15 \pmod{26}$ has a unique solution modulo 26, and step 2 is not applicable. Then

$$\begin{aligned}
 9x \equiv 15 \pmod{26} &\iff 3x \equiv 5 \pmod{26}, && \text{by step 3,} \\
 &\iff 27x \equiv 45 \pmod{26}, && \text{by step 5,} \\
 &&& \text{multiplying by 9,} \\
 &\iff x \equiv 45 \pmod{26}, && \text{by step 4,} \\
 &\iff x \equiv 19 \pmod{26}, && \text{by step 4.}
 \end{aligned}$$

The steps that we followed in this worked exercise are certainly not unique. There are many ways of solving the congruence, but, of course, all must lead to the same conclusion.

Exercise 3.3

Solve the following linear congruences.

- (a) $28x \equiv 49 \pmod{53}$
- (b) $34x \equiv 19 \pmod{52}$
- (c) $137x \equiv 96 \pmod{19}$
- (d) $51x \equiv 8 \pmod{53}$
- (e) $18x \equiv 39 \pmod{69}$

Exercise 3.4

- (a) Solve the following linear congruences.
 - (i) $8x \equiv 12 \pmod{60}$
 - (ii) $21x \equiv 35 \pmod{47}$
 - (iii) $6x \equiv 5 \pmod{41}$
 - (iv) $5x \equiv 1 \pmod{93}$
- (b) Solve the following polynomial congruences.
 - (i) $x^3 \equiv 1 \pmod{7}$
 - (ii) $2x^2 + 4x + 5 \equiv 0 \pmod{7}$
- (c) Use congruences to solve the following linear Diophantine equations.
 - (i) $12x + 19y = 7$
 - (ii) $17x + 41y = 13$
- (d) There are 19×20 congruences of the form $ax \equiv b \pmod{20}$, since there are 19 different choices for $a \not\equiv 0 \pmod{20}$ and 20 choices for b .

For how many of these congruences does a solution exist, and for how many congruences is the solution unique?

4 Simultaneous linear congruences

Now we have seen how to solve linear congruences, we will explore the theory that allows us to solve *simultaneous* linear congruences.

4.1 The Chinese Remainder Theorem

In the first century AD the Chinese mathematician Sun Tzu posed the following problem.

Worked Exercise 4.1

Find a number that leaves remainders 2, 3 and 2 when divided by 3, 5 and 7 respectively.

Solution

In congruence notation the problem is asking for a simultaneous solution of the system

$$x \equiv 2 \pmod{3}; \quad x \equiv 3 \pmod{5}; \quad x \equiv 2 \pmod{7}.$$

We can solve this problem as follows. To satisfy the first congruence x must be of the form $3r + 2$. To satisfy the second congruence as well requires

$$3r + 2 \equiv 3 \pmod{5}, \quad \text{that is,} \quad 3r \equiv 1 \pmod{5}.$$

This has the unique solution $r \equiv 2 \pmod{5}$, that is, $r = 5s + 2$ for some integer s . Therefore

$$x = 3r + 2 = 3(5s + 2) + 2 = 15s + 8.$$

This number has to satisfy the third and final congruence:

$$15s + 8 \equiv 2 \pmod{7} \iff s + 1 \equiv 2 \pmod{7}.$$

This has the unique solution $s \equiv 1 \pmod{7}$. So $s = 7t + 1$ for some integer t and, substituting into the expression for x ,

$$x = 15(7t + 1) + 8 = 105t + 23.$$

Any integer x of this form satisfies all three congruences. The least positive solution is 23 (corresponding to $t = 0$) and the complete solution is $x \equiv 23 \pmod{105}$.

By ‘simultaneous solution’ we mean an x that satisfies *all* the congruences.

Consider now a general **system of simultaneous linear congruences** to be solved, that is, a system

$$a_1x \equiv b_1 \pmod{n_1}; a_2x \equiv b_2 \pmod{n_2}; \dots; a_rx \equiv b_r \pmod{n_r}.$$

For an integer x to be a **simultaneous solution** of the system it must be a solution of each of the r individual congruences, and consequently a necessary condition for a solution is that

$$\text{hcf}(a_i, n_i) \text{ divides } b_i, \quad \text{for each } i = 1, 2, \dots, r.$$

Assuming that this condition holds, a first step in solving the simultaneous system is to solve each individual congruence, finding its unique solution for the appropriate modulus. We can do this by applying the strategy for solving linear congruences given in the previous section, leading to congruences in which the coefficient of x is 1. So from then on we can confine attention to solving simultaneous systems of the form

$$x \equiv b_1 \pmod{n_1}; x \equiv b_2 \pmod{n_2}; \dots; x \equiv b_r \pmod{n_r}$$

as in Sun Tzu's problem.

The fact that each congruence is solvable is not sufficient on its own for the simultaneous system to have a solution. For example, consider the following system:

$$x \equiv 1 \pmod{2}; x \equiv 2 \pmod{4}.$$

No even integer satisfies the first congruence and no odd integer satisfies the second; hence the simultaneous system has *no* solutions.

Inconsistencies, such as the one illustrated here, can arise when two linear congruences have moduli that are not coprime. However, if we restrict ourselves to systems in which every pair of moduli is coprime, it turns out that simultaneous solutions always exist.

Theorem 4.2 Chinese Remainder Theorem

Let $n_1, n_2, \dots, n_r$ be natural numbers such that $\text{hcf}(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv b_1 \pmod{n_1}; x \equiv b_2 \pmod{n_2}; \dots; x \equiv b_r \pmod{n_r}$$

has a simultaneous solution that is unique modulo $n_1n_2 \cdots n_r$.

The moduli $n_1, n_2, \dots, n_r$ are said to be pairwise coprime.

Proof We prove the theorem by first constructing a solution and then showing that it is unique modulo $n_1n_2 \cdots n_r$.

Let $N = n_1n_2 \cdots n_r$ and $N_k = \frac{N}{n_k}$, for $k = 1, 2, \dots, r$. Then, since $\text{hcf}(n_i, n_k) = 1$ for each $i \neq k$, it follows that

$$\text{hcf}(N_k, n_k) = \text{hcf}(n_1n_2 \cdots n_{k-1}n_{k+1} \cdots n_r, n_k) = 1,$$

and so the linear congruence $N_kx \equiv 1 \pmod{n_k}$ has a unique solution modulo n_k . Let this solution be x_k , so $N_kx_k \equiv 1 \pmod{n_k}$.

We will show that the integer

$$x_0 = b_1 N_1 x_1 + b_2 N_2 x_2 + \cdots + b_r N_r x_r$$

satisfies each of the congruences. To achieve this we evaluate x_0 modulo n_k , for each $k = 1, 2, 3, \dots, r$.

We start by noting that, whenever $i \neq k$, since n_k divides N_i , we have $N_i \equiv 0 \pmod{n_k}$. Consequently

$$x_0 \equiv b_k N_k x_k \pmod{n_k}, \quad \text{for each } k = 1, 2, \dots, r,$$

as each of the remaining terms in the sum is congruent to 0 modulo n_k .

Finally, since x_k was found such that $N_k x_k \equiv 1 \pmod{n_k}$, we have

$$x_0 \equiv b_k \pmod{n_k}$$

as claimed.

It remains to show that the discovered solution is unique modulo the product $n_1 n_2 \cdots n_r$. To this end suppose that x' is a second simultaneous solution of the system, that is,

$$x_0 \equiv x' \equiv b_k \pmod{n_k}, \quad \text{for each } k = 1, 2, \dots, r.$$

This implies that each n_k divides $x' - x_0$, whereupon the fact that the moduli are pairwise coprime gives us by Lemma 4.11 of Chapter 1 that

$$n_1 n_2 \cdots n_r \text{ divides } x' - x_0.$$

This amounts to

$$x' \equiv x_0 \pmod{n_1 n_2 \cdots n_r}$$

exactly as required. ■

To illustrate the proof of the Chinese Remainder Theorem, we trace its steps in an example.

Worked Exercise 4.3

Solve the system of simultaneous linear congruences

$$x \equiv 5 \pmod{6}; \quad x \equiv 4 \pmod{11}; \quad x \equiv 3 \pmod{17}.$$

Solution

The given values of the variables in the proof are

$$\begin{aligned} \text{coefficients: } & b_1 = 5, \quad b_2 = 4, \quad b_3 = 3; \\ \text{moduli: } & n_1 = 6, \quad n_2 = 11, \quad n_3 = 17. \end{aligned}$$

The calculated values are

$$\begin{aligned} N &= 6 \times 11 \times 17 = 1122, \quad N_1 = 11 \times 17 = 187, \\ N_2 &= 6 \times 17 = 102, \quad N_3 = 6 \times 11 = 66. \end{aligned}$$

The values x_i are obtained by solving the linear congruences $N_i x \equiv 1 \pmod{n_i}$.

$$\begin{aligned} N_1 x \equiv 1 \pmod{n_1} &\iff 187x \equiv 1 \pmod{6} \\ &\iff x \equiv 1 \pmod{6}; \text{ so } x_1 = 1. \\ N_2 x \equiv 1 \pmod{n_2} &\iff 102x \equiv 1 \pmod{11} \\ &\iff 3x \equiv 1 \pmod{11} \\ &\iff x \equiv 4 \pmod{11}; \text{ so } x_2 = 4. \\ N_3 x \equiv 1 \pmod{n_3} &\iff 66x \equiv 1 \pmod{17} \\ &\iff -2x \equiv -16 \pmod{17} \\ &\iff x \equiv 8 \pmod{17}; \text{ so } x_3 = 8. \end{aligned}$$

Therefore

$$\begin{aligned} x_0 &= 5 \times 187 \times 1 + 4 \times 102 \times 4 + 3 \times 66 \times 8 = 4151 \\ &\equiv 785 \pmod{1122}. \end{aligned}$$

Exercise 4.1

Find the least natural number n such that 3^2 divides $2n + 3$, 4^2 divides $3n + 4$ and 5^2 divides $4n + 5$.

4.2 Solving simultaneous congruences

One situation in which a system of simultaneous linear congruences can be introduced is when confronted with the problem of solving a single linear congruence in which the modulus is large and composite. To see how this works, let n have prime decomposition $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ and compare the linear congruence

$$ax \equiv b \pmod{n}$$

and the system

$$ax \equiv b \pmod{p_1^{k_1}}; \quad ax \equiv b \pmod{p_2^{k_2}}; \quad \dots; \quad ax \equiv b \pmod{p_r^{k_r}}.$$

Certainly any integer x that satisfies $ax \equiv b \pmod{n}$ also satisfies each congruence in the system, because $p_i^{k_i}$ divides n for each i . On the other hand, since the p_i are pairwise coprime, repeated use of Corollary 1.7 of this chapter tells us that any solution of the simultaneous system must satisfy $ax \equiv b \pmod{n}$. So the two are equivalent.

We will solve a problem of this sort in Worked Exercise 4.4. However, in this exercise we abandon the formal approach of Worked Exercise 4.3 and Exercise 4.1, in which we traced the explicit construction of a solution as given in the proof of the Chinese Remainder Theorem. The method that we adopt here, like our solution of Sun Tzu's problem at the beginning of the section, will not require the same amount of careful arithmetic. Indeed, we often treat the Chinese Remainder Theorem as an important theoretical result that confirms the existence of solutions, but apply other methods, such as the one we are about to illustrate, to discover what those solutions are.

Worked Exercise 4.4

Solve the linear congruence $3x \equiv 5 \pmod{1001}$.

Solution

Observing that $1001 = 7 \times 11 \times 13$, we seek the simultaneous solution of

$$3x \equiv 5 \pmod{7}; \quad 3x \equiv 5 \pmod{11}; \quad 3x \equiv 5 \pmod{13}.$$

That is (having first solved each of these congruences individually),

$$x \equiv 4 \pmod{7}; \quad x \equiv 9 \pmod{11}; \quad x \equiv 6 \pmod{13}.$$

The natural numbers x that satisfy the congruence $x \equiv 6 \pmod{13}$ are

$$x = 6, 19, 32, 45, 58, 71, 84, 97, \dots$$

Now 97 is the first of these integers that is congruent to 9 modulo 11, and consequently, $x \equiv 97 \pmod{11 \times 13}$ is the unique solution of the final pair of congruences of the system. The natural numbers in this solution set are

$$x = 97, 240, 383, 526, 669, \dots$$

Now 669 is the first of these that is also congruent to 4 modulo 7, and hence is the smallest natural number satisfying all three congruences. Hence

$$x \equiv 669 \pmod{7 \times 11 \times 13}$$

is the unique solution of the congruence. This method is illustrated in Figure 4.1.

Note that the numbers satisfying one congruence also form a pattern with respect to the next congruence in the system. For instance,

$$\begin{aligned} x &= 6, 19, 32, 45, 58, 71, 84, \dots \\ &\equiv 6, 8, 10, 1, 3, 5, 7, \dots \pmod{11}. \end{aligned}$$

Examining this pattern, it is possible to see quite quickly where the solution that is congruent to 9 modulo 11 is going to fall.

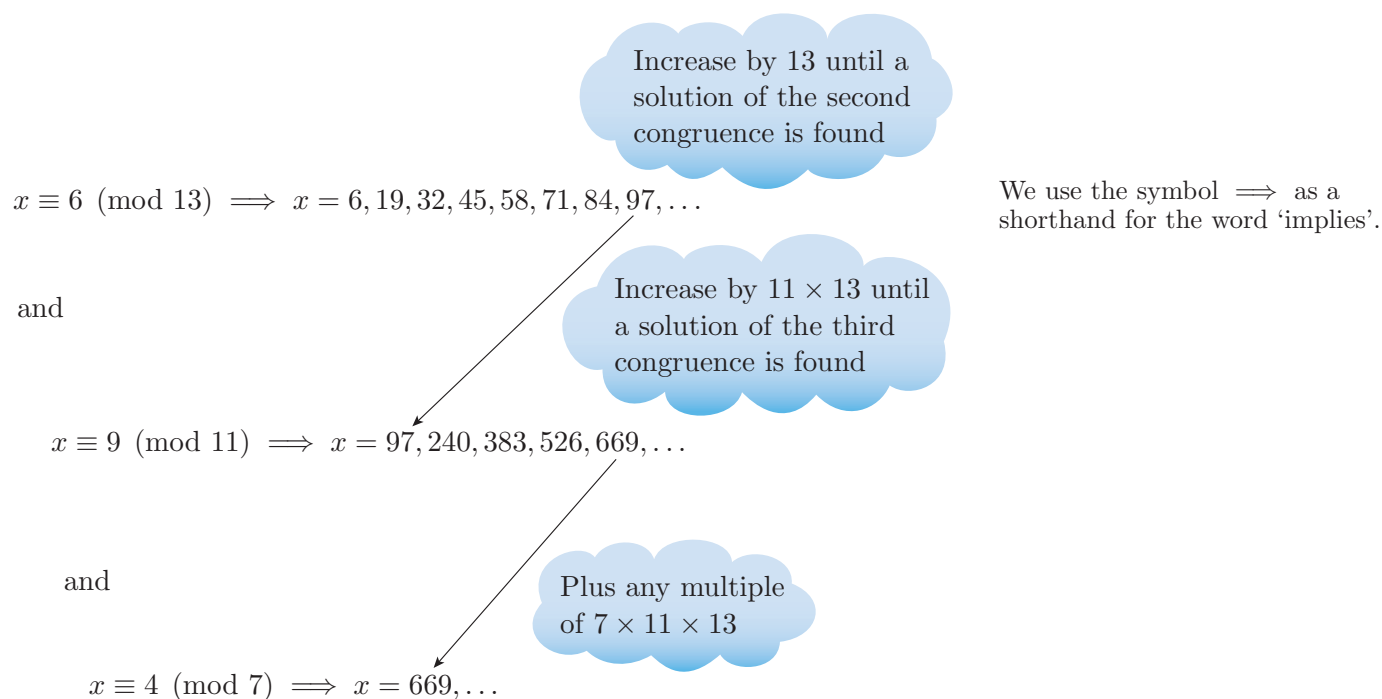


Figure 4.1 Solving simultaneous linear congruences

Exercise 4.2

Solve the linear congruence $7x \equiv 9 \pmod{165}$.

There remains one loose end to tidy up. We have seen that when a system of linear congruences has moduli that are not pairwise coprime, the system may be inconsistent and have no solutions. But this is not necessarily the case. For instance, the system

$$x \equiv 2 \pmod{6}; \quad x \equiv 5 \pmod{9}$$

involves moduli that are not pairwise coprime. However, $x = 14$ certainly satisfies both congruences, and so solutions do exist.

Theorem 4.5

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}$$

has a simultaneous solution if, and only if, $\text{hcf}(n_1, n_2)$ divides $b_2 - b_1$. If a solution exists then it is unique modulo $\text{lcm}(n_1, n_2)$.

Proof Suppose that the integer x satisfies both

$$x \equiv b_1 \pmod{n_1} \quad \text{and} \quad x \equiv b_2 \pmod{n_2}.$$

That is, there exist integers r and s such that

$$x - b_1 = n_1 r \quad \text{and} \quad x - b_2 = n_2 s.$$

Eliminating x from this pair of equations leads to

$$b_2 - b_1 = n_1 r - n_2 s.$$

Now the right-hand side is an integer combination of n_1 and n_2 and, as such, is a multiple of $\text{hcf}(n_1, n_2)$. Thus $\text{hcf}(n_1, n_2)$ divides $b_2 - b_1$, and so this is a necessary condition for the system to have a solution.

To confirm that the condition is sufficient to guarantee a solution, we reverse the argument. Suppose that

$$b_2 - b_1 = k \text{hcf}(n_1, n_2), \quad \text{for some integer } k.$$

Now we know that there exist integers u and v such that

$$\text{hcf}(n_1, n_2) = un_1 + vn_2.$$

Elimination of $\text{hcf}(n_1, n_2)$ from this pair of equations produces

$$b_1 + kun_1 = b_2 - kvn_2.$$

Then

$$b_1 + kun_1 = b_1 + (ku)n_1 \equiv b_1 \pmod{n_1}$$

and

$$b_1 + kun_1 = b_2 - (kv)n_2 \equiv b_2 \pmod{n_2}.$$

So $b_1 + kun_1$ satisfies both congruences and confirms that simultaneous solutions do exist.

Finally, there is the question of uniqueness. Suppose that x_1 and x_2 are two solutions. That is,

$$x_1 \equiv x_2 \equiv b_1 \pmod{n_1} \quad \text{and} \quad x_1 \equiv x_2 \equiv b_2 \pmod{n_2}.$$

Theorem 1.6 of this chapter now completes the task:

$$x_1 \equiv x_2 \pmod{\text{lcm}(n_1, n_2)}. \quad \blacksquare$$

The result of Theorem 4.5 can be generalised to cover any number of congruences. A proof using mathematical induction is readily available but is omitted here as the details are somewhat tedious.

Corollary 4.6

The system of linear congruences

$$x \equiv b_1 \pmod{n_1}; \quad x \equiv b_2 \pmod{n_2}; \quad \dots; \quad x \equiv b_r \pmod{n_r}$$

has a simultaneous solution if, and only if, $\text{hcf}(n_i, n_j)$ divides $b_j - b_i$ for each pair i, j of suffixes. If a solution exists it is unique modulo $\text{lcm}(n_1, n_2, \dots, n_r)$.

Exercise 4.3

For each of the following systems of simultaneous linear congruences, decide whether or not it has solutions and, if so, solve the system.

(a) $x \equiv 7 \pmod{12}; \quad x \equiv 11 \pmod{18}; \quad x \equiv 1 \pmod{23}$

(b) $x \equiv 4 \pmod{12}; \quad x \equiv 10 \pmod{18}; \quad x \equiv 3 \pmod{7}$

Throughout the remainder of the topic we will continue to meet congruence problems. It may be surprising how often the task of solving linear congruences crops up in the context of deeper problems.

The final exercise in this chapter gives you some further practice at solving congruence problems.

Exercise 4.4

- (a) Solve the following system of congruences by following the steps in the proof of the Chinese Remainder Theorem.

$$x \equiv 1 \pmod{4}; \quad x \equiv 3 \pmod{5}; \quad x \equiv 0 \pmod{7}$$

- (b) Solve the following systems of congruences by any method.

(i) $2x \equiv 3 \pmod{5}; \quad 3x \equiv 4 \pmod{7}; \quad 4x \equiv 9 \pmod{11}$

(ii) $x \equiv 1 \pmod{4}; \quad x \equiv 3 \pmod{6}; \quad x \equiv 3 \pmod{9}$

- (c) Solve the following linear congruence.

$$19x \equiv 7 \pmod{2310}$$

- (d) Find the smallest natural number n such that 3^2 divides n , 4^2 divides $n + 1$ and 5^2 divides $n + 2$.

- (e) In the arithmetic progression

$$7, 18, 29, 40, 51, \dots$$

find the first three consecutive terms that are divisible by 2, 3 and 5 respectively (that is, the first of the three consecutive terms is divisible by 2, the second is divisible by 3 and the third is divisible by 5).

- (f) For which values of c does the following system of congruences have a simultaneous solution?

$$5x \equiv c \pmod{12}; \quad 7x \equiv 2 \pmod{30}$$

- (g) A band of seventeen pirates stole a sack of gold coins. On attempting to divide the spoils into equal portions, they found that four coins were left over. A brawl over who should get the extra coins followed and one pirate was killed. When the spoils were redistributed amongst the survivors, ten coins were left over. Again an argument developed and one pirate was killed. But now the spoils divided equally between the remaining pirates. What was the least number of coins that could have been stolen?

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should:

- (a) Understand the meaning of the terms ‘congruence’ and ‘residue class’, and be confident in using these to manipulate expressions in modular arithmetic.
- (b) Recognise and be able to use the connection between divisibility tests and congruence.
- (c) Be able to distinguish between distinct solutions of polynomial congruences, and apply basic methods to solve basic polynomial congruences with low modulus.
- (d) Be able to use divisibility tests, in particular those for divisibility by 9 and 11, and explain why they work.
- (e) Understand the proof of the solution of linear congruences, and be able to apply the theory to specific examples.
- (f) Recall and be able to apply the strategy to solve linear congruences, and use this to solve certain linear Diophantine equations.
- (g) Understand the statement, proof and applications of the Chinese Remainder Theorem.
- (h) Be able to use a range of techniques to solve simultaneous linear congruences.

Solutions to exercises

Solution to Exercise 1.1

- (a) False, as $3 - 29 = -26$, which is not a multiple of 8.
- (b) True, as $3 - (-29) = 32 = 4 \times 8$.
- (c) True, as $63 - 37 = 26 = 2 \times 13$.
- (d) True, as $37 - 63 = -26 = (-2) \times 13$.
- (e) True, as $63 - 63 = 0 = 0 \times 37$.
- (f) False, as $63 - 13 = 50 = 2 \times 25$, so $63 \equiv 13 \pmod{25}$.

From the definition of factors (Definition 4.3 of Chapter 1), 0 is divisible by every natural number.

Solution to Exercise 1.2

Since $a \equiv b \pmod{n}$, let k be the integer such that $a - b = kn$.

- (a) As m divides n we have $n = mr$ for some integer r . Therefore

$$a - b = kn = k(mr) = (kr)m,$$

which confirms that $a \equiv b \pmod{m}$.

- (b) Multiplying by m gives

$$\begin{aligned} ma - mb &= mkn = k(mn), & \text{confirming } ma &\equiv mb \pmod{mn}, \\ &= (mk)n, & \text{confirming } ma &\equiv mb \pmod{n}. \end{aligned}$$

- (c) Dividing by d gives

$$\frac{a}{d} - \frac{b}{d} = k\frac{n}{d}, \quad \text{in which } \frac{a}{d}, \frac{b}{d} \text{ and } \frac{n}{d} \text{ are integers.}$$

This implies that $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

- (d) Let $\text{hcf}(a, n) = d_1$ and $\text{hcf}(b, n) = d_2$. Since d_1 divides a , and d_1 divides n , it follows that d_1 divides $a - kn$; that is, d_1 divides b . But then d_1 is a common factor of b and n , and so $d_1 \leq d_2$.

On the other hand, d_2 divides b , and d_2 divides n , giving d_2 divides $b + kn$; that is, d_2 divides a . So d_2 is a common factor of a and n , and so $d_2 \leq d_1$. Hence the equality $d_1 = d_2$ follows.

- (e) Here $(a + c) - (b + c) = a - b = kn$, and so $a + c \equiv b + c \pmod{n}$.

Note that the result in part (e) is just a special, but important, case of Theorem 1.2(d) in which $d = c$.

Solution to Exercise 1.3

- (a) (i) The set of least positive residues modulo 10 is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

The set of least absolute residues modulo 10 is

$$\{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

- (ii) The set of least positive residues modulo 11 is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

The set of least absolute residues modulo 11 is

$$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}.$$

- (b) (i) Replacing each of the numbers by the least positive residue to which it is congruent modulo 11 (for instance
- $-3 \equiv 8$
- ,
- $22 \equiv 0$
- , etc.), we obtain

$$\{6, 2, -3, 22, 23, -7, 7, 9, 43, -8, 16\} \equiv \{6, 2, 8, 0, 1, 4, 7, 9, 10, 3, 5\}.$$

As the latter is the set of least positive residues modulo 11, the former is a complete set of residues modulo 11.

- (ii) As
- $10^2 = 100 \equiv 1$
- and
- $1^2 \equiv 1 \pmod{11}$
- , the eleven numbers do not form a complete set of residues. In fact only six residue classes are represented in this set, as
- $9^2 \equiv 2^2$
- ,
- $8^2 \equiv 3^2$
- ,
- $7^2 \equiv 4^2$
- and
- $6^2 \equiv 5^2$
- .

- (iii) Starting from 1, each subsequent number is obtained by doubling. To avoid calculation of high powers of 2, we can write down the least positive residue for each of the numbers by systematically ‘doubling modulo 11’. The given eleven numbers are congruent, in order, to the following numbers modulo 11:

$$0, 1, 2, 4, 8, 16 \equiv 5, 10, 20 \equiv 9, 18 \equiv 7, 14 \equiv 3, 6.$$

As these numbers form the set of least positive residues modulo 11, the given set is a complete set of residues.

When there is no ambiguity over which modulus is involved we will occasionally, as in this solution, use the $\equiv$ symbol without its accompanying $(\text{mod } n)$.

Each time 11 is exceeded, the number is replaced by the least positive residue and doubling begins again.

Solution to Exercise 1.4

In $\mathbb{Z}_{10}$:

$$[6] + [8] = [6 + 8] = [14] = [4], \text{ since } 14 \equiv 4 \pmod{10}.$$

$$[6] \times [8] = [6 \times 8] = [48] = [8], \text{ since } 48 \equiv 8 \pmod{10}.$$

Allowing b to take each of the values $0, 1, 2, \dots, 9$ in turn, we find that the corresponding values of $[6] \times [b]$ are $[0], [6], [2], [8], [4], [0], [6], [2], [8]$ and $[4]$. So $[6] \times [b] = [8]$ has the two solutions $[b] = [3]$ and $[b] = [8]$.

Repeating in $\mathbb{Z}_{11}$:

$$[6] + [8] = [14] = [3], \text{ since } 14 \equiv 3 \pmod{11}.$$

$$[6] \times [8] = [48] = [4], \text{ since } 48 \equiv 4 \pmod{11}.$$

$$[6] \times [b] = [8] \text{ has the unique solution } [b] = [5].$$

Solution to Exercise 1.5

- (a) We first note that if $n \geq 7$ then 7 divides $n!$ and so $n! \equiv 0 \pmod{7}$. Therefore we have the simplification

$$1! + 2! + 3! + \cdots + 1000! \equiv 1! + 2! + 3! + \cdots + 6! \pmod{7}$$

(which removes all fear of the problem!). Now, working modulo 7, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24 \equiv 3$, $5! = 5 \times 4! \equiv 5 \times 3 \equiv 1$ and $6! = 6 \times 5! \equiv 6 \times 1 = 6$. And so,

$$1! + 2! + 3! + \cdots + 1000! \equiv 1 + 2 + 6 + 3 + 1 + 6 = 19 \equiv 5 \pmod{7},$$

and the remainder on dividing by 7 is 5.

- (b) $a^2 - 1$ is divisible by 24 precisely when $a^2 - 1 \equiv 0 \pmod{24}$ or equivalently, adding 1 to both sides and appealing to Theorem 1.2(d), when $a^2 \equiv 1 \pmod{24}$. So our task is to show that any integer a that is divisible neither by 2 nor by 3 must satisfy $a^2 \equiv 1 \pmod{24}$.

The Division Algorithm tells us that a can be written as

$$a = 24q + r, \text{ where } 0 \leq r < 24.$$

But, written in this way, a is divisible by 2 when r is even, and is divisible by 3 when r is divisible by 3. There are just eight values of r that are not divisible by either 2 or 3, namely $r = 1, 5, 7, 11, 13, 17, 19$ and 23. For a to be not divisible by either 2 or 3 it must be congruent to one of these eight values modulo 24. Thus we have, on replacing each of the last four listed values by its least absolute residue,

$$a \equiv \pm 1, \pm 5, \pm 7 \text{ or } \pm 11 \pmod{24}.$$

Now appealing to Theorem 1.2(f) gives

$$a^2 \equiv 1, 25, 49 \text{ or } 121 \pmod{24}.$$

But each of these numbers has remainder 1 when divided by 24, and the result follows.

Solution to Exercise 1.6

- (a) We wish to cancel the common factor 6. As $\text{hcf}(6, 30) = 6$, we also divide the modulus by 6:

$$6x \equiv 18 \pmod{30} \iff x \equiv 3 \pmod{5}.$$

- (b) In order to cancel the common factor 10, the modulus has to be divided by $\text{hcf}(10, 45) = 5$. So

$$20x \equiv 30 \pmod{45} \iff 2x \equiv 3 \pmod{9}.$$

- (c) The common factor 13 can be cancelled without adjustment to the modulus, since $\text{hcf}(13, 60) = 1$. So

$$52x \equiv 39 \pmod{60} \iff 4x \equiv 3 \pmod{60}.$$

Solution to Exercise 1.7

- (a) (i) Since $1997 = 7 \times 285 + 2$,
the least positive residue is 2, and
the least absolute residue is 2.
- (ii) Since $1997 = 17 \times 117 + 8$,
the least positive residue is 8, and
the least absolute residue is 8.
- (iii) Since $1997 = 101 \times 19 + 78$,
the least positive residue is 78, and
the least absolute residue is $78 - 101 = -23$.
- (b) If $k \equiv 1 \pmod{12}$ then $k = 12r + 1$, for some integer r . Hence
 $6k + 5 = 72r + 11$.
- (i) As 4 divides 72, we have $6k + 5 \equiv 11 \equiv 3 \pmod{4}$, and so 3 is the
required least positive residue.
- (ii) As 9 divides 72, we have $6k + 5 \equiv 11 \equiv 2 \pmod{9}$, and so 2 is the
required least positive residue.
- (iii) As 12 divides 72, we have $6k + 5 \equiv 11 \pmod{12}$, and so 11 is the
required least positive residue.
- (c) (i) $1^2 \equiv 6^2 \pmod{7}$ but it is not the case that $1 \equiv 6 \pmod{7}$.
- (ii) $1^2 \equiv 2^2 \pmod{3}$ and $2 \equiv 5 \pmod{3}$, but $1^5 \not\equiv 2^5 \pmod{3}$.
- (d) Let $P(n)$ be the proposition that $6^n \equiv 5n + 1 \pmod{25}$.
 $P(1)$ claims that $6 \equiv 6 \pmod{25}$, which is trivially true. We continue
by assuming that $P(k)$ is true and investigate $P(k + 1)$.

$$\begin{aligned}
 6^{k+1} &= 6 \times 6^k \equiv 6 \times (5k + 1), \quad \text{by the induction hypothesis,} \\
 &\equiv 30k + 6 \pmod{25} \\
 &\equiv 5k + 6 \pmod{25} \\
 &\equiv 5(k + 1) + 1 \pmod{25},
 \end{aligned}$$

as required.

Hence the Principle of Mathematical Induction confirms that $P(n)$ is
true for all integers $n \geq 1$.

- (e) The set of n numbers will form a complete set of residues modulo n
provided no two of them are congruent modulo n . So, aiming for a
contradiction, suppose that two of the numbers are congruent
modulo n , say

$$c + ra \equiv c + sa \pmod{n}, \text{ where } 0 \leq s < r < n.$$

The definition of congruence would then give

$$n \text{ divides } (c + ra) - (c + sa).$$

That is,

$$n \text{ divides } (r - s)a.$$

But $\text{hcf}(a, n) = 1$, and so Euclid's Lemma leads to

$$n \text{ divides } r - s,$$

which is impossible since $0 < r - s < n$.

- (f) There is no unique set of steps to answer these questions. You might well have found different ways of grouping the terms from those in the solutions that follow.

- (i) As $11 \equiv 4 \pmod{7}$, we have $11^{11} \equiv 4^{11} \pmod{7}$.

Now $4^2 = 16 \equiv 2 \pmod{7}$ and so

$$11^{11} \equiv 4^{11} = (4^2)^5 \times 4 \equiv 2^5 \times 4 = 32 \times 4 \equiv 4 \times 4 \equiv 2 \pmod{7}.$$

So the remainder is 2.

- (ii) As $11^2 = 121 \equiv 2 \pmod{17}$, we have

$$11^{11} = (11^2)^5 \times 11 \equiv 2^5 \times 11 \equiv (-2) \times 11 \equiv -5 \equiv 12 \pmod{17}.$$

So the remainder is 12.

- (iii) We have

$$\begin{aligned} 11^{11} &\equiv (-8)^{11} = ((-8)^2)^5 \times (-8) \equiv 7^5 \times (-8) \pmod{19} \\ &= 7^2 \times 7^2 \times 7 \times (-8) \equiv 11 \times 11 \times (-56) \pmod{19} \\ &\equiv (-8)^2 \times 1 = 64 \equiv 7 \pmod{19}. \end{aligned}$$

So the remainder is 7.

- (g) (i) We have

$$\begin{aligned} 2^{28} &= (2^5)^5 \times 2^3 \equiv 3^5 \times 2^3 = 27 \times 9 \times 8 \pmod{29} \\ &\equiv (-2) \times 14 = -28 \equiv 1 \pmod{29}, \end{aligned}$$

which amounts to saying that 29 divides $2^{28} - 1$.

- (ii) We have

$$\begin{aligned} 3^{39} &= (3^4)^9 \times 3^3 \equiv 2^9 \times 3^3 = (8 \times 9) \times (32 \times 3) \pmod{79} \\ &\equiv (-7) \times (17) \times 2 = (-119) \times 2 \pmod{79} \\ &\equiv (-40) \times 2 = -80 \equiv -1 \pmod{79}. \end{aligned}$$

It follows that 79 divides $3^{39} + 1$.

- (h) First note that any square is congruent to either 0 or 1 modulo 3 because $0^2 \equiv 0$, $1^2 \equiv 1$ and $2^2 \equiv 1 \pmod{3}$. From this follows that $a^2 + 3b^2$ is congruent to either 0 or 1 modulo 3 since $3b^2 \equiv 0 \pmod{3}$. But $3k - 1 \equiv 2 \pmod{3}$, and so $a^2 + 3b^2$ cannot be equal to $3k - 1$ for any integer k , regardless of whether or not it is prime.
- (i) The congruences $ar \equiv b \pmod{n}$ and $cr \equiv d \pmod{n}$ tell us that there exist integers k and s such that $ar - b = kn$ and $cr - d = sn$. Substituting for b from the first of these equations and for d from the second gives

$$ad - bc = a(cr - sn) - (ar - kn)c = n(kc - as),$$

which shows that $ad \equiv bc \pmod{n}$.

Solution to Exercise 2.1

(a) (i) We have

$$N \equiv 9 + 7 + 2 + 3 \equiv 3 \pmod{9},$$

$$M \equiv 1 + 8 + 0 + 5 + 6 \equiv 2 \pmod{9},$$

$$N + M \equiv 3 + 2 \equiv 5 \pmod{9},$$

$$N - M \equiv 3 - 2 \equiv 1 \pmod{9}.$$

Hence the required remainders are 3, 2, 5 and 1 respectively.

(ii) We have

$$N \equiv 3 - 2 + 7 - 9 = -1 \equiv 10 \pmod{11},$$

$$M \equiv 6 - 5 + 0 - 8 + 1 = -6 \equiv 5 \pmod{11},$$

$$N + M \equiv 10 + 5 \equiv 4 \pmod{11},$$

$$N - M \equiv 10 - 5 \equiv 5 \pmod{11}.$$

Hence the required remainders are 10, 5, 4 and 5 respectively.

(iii) $N \times M \equiv 3 \times 2 \equiv 6 \pmod{9}$, and so the number on the right-hand side of the equation has to be congruent to 6 modulo 9.

$$1 + 7 + 5 + (?) + 5 + 8 + 4 + 8 + 8 = 46 + (?) \equiv 1 + (?) \equiv 6 \pmod{9},$$

from which it follows that the missing digit (?) can only be 5.

(b) Let $N = a_{2m-1}a_{2m-2} \dots a_2a_1a_0$ so that $M = a_0a_{2m-1}a_{2m-2} \dots a_2a_1$. Since N and M comprise the same $2m$ digits, the 9-test gives

$$N \equiv M \equiv a_0 + a_1 + a_2 + \dots + a_{2m-2} + a_{2m-1} \pmod{9},$$

and so $N - M \equiv 0 \pmod{9}$, that is, 9 divides $N - M$.

Applying the 11-test:

$$N \equiv a_0 - a_1 + a_2 - \dots + a_{2m-2} - a_{2m-1} \pmod{11}$$

whilst

$$M \equiv a_1 - a_2 + a_3 - \dots - a_{2m-2} + a_{2m-1} - a_0 \pmod{11}.$$

So $N + M \equiv 0 \pmod{11}$. That is, 11 divides $N + M$.

Finally, since $N^2 - M^2 = (N - M)(N + M)$ we have that 9 divides $N^2 - M^2$ and 11 divides $N^2 - M^2$. As $\text{hcf}(9, 11) = 1$, Corollary 1.7 allows us to conclude that 99 divides $N^2 - M^2$.

Solution to Exercise 2.2

- (a) (i) As 108 is divisible by 9, the right-hand side must be divisible by 9. Hence, adding up the digits, $4 + 0 + 0 + (?) + 8 \equiv 0 \pmod{9}$ and the only value of the digit $(?)$ that renders this possible is 6.

- (ii) Checking the calculation modulo 9,

$$1578 \times 34971 \equiv 3 \times 6 \equiv 0 \pmod{9},$$

and so the sum of the digits on the right-hand side must be divisible by 9. Thus

$$5 + 5 + 1 + 8 + (?) + 2 + 3 + 8 = 32 + (?) \equiv 5 + (?) \equiv 0 \pmod{9},$$

giving $(?) = 4$.

- (iii) The right-hand side is divisible by 11 because

$7 - 8 + 8 - 6 + 2 - 4 + 1 \equiv 0 \pmod{11}$, and so the left-hand side must be divisible by 11. Now 4473 is not divisible by 11, and so $3(?)9$ must be; that is, $9 - (?) + 3 \equiv 0 \pmod{11}$. Hence $(?) = 1$ is the only possibility.

- (b) Aiming for a contradiction, suppose that A divides B , say $B = nA$ for some integer n . Now as A comprises the digits 1 to 7, we have

$$A \equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 = 28 \equiv 1 \pmod{9}$$

and similarly $B \equiv 1 \pmod{9}$.

Since $A \equiv B \equiv 1 \pmod{9}$, the equation $B = nA$ then gives $n \equiv 1 \pmod{9}$. Because A is not equal to B , we must have $n \geq 10$. However, this is impossible since it forces B to have more digits than A . This contradiction shows that no such n can exist and so A does not divide B .

- (c) The key here is to note that, as M and N have the same collection of digits, $N \equiv M \pmod{9}$ or, what amounts to the same thing, $N - M \equiv 0 \pmod{9}$. But X is the sum of the digits of $N - M$ and so $X \equiv 0 \pmod{9}$. Now $N - M$ is a number with ten (or fewer) digits and so $X \leq 90$. Of all numbers not exceeding 90, the maximum sum of the digits is 17 (achieved by the number 89). X cannot be equal to 0 as that would happen if, and only if, $N = M$.

Let Y be the sum of the digits of X . Then

$$Y \equiv X \equiv 0 \pmod{9}, \quad \text{where } 0 < Y < 18.$$

Thus the only possibility is $Y = 9$.

- (d) On dividing N by 10^n , the Division Algorithm gives integers q and r such that

$$N = 10^n q + r, \quad 0 \leq r < 10^n.$$

Because of the restriction on r , it follows that r is the number made up of the last n digits of N .

Now 2^n divides 10^n and so, taking congruence modulo 2^n ,

$$N \equiv r \pmod{2^n}.$$

For example, to extract the final three digits from 1234567 we write
 $1234567 = 1234 \times 10^3 + 567$.

Thus $N \equiv 0 \pmod{2^n}$ if, and only if, $r \equiv 0 \pmod{2^n}$; that is, 2^n divides N if, and only if, 2^n divides r , the number made up of the last n digits of N .

(e) (i) We have

$$\begin{aligned} 10^{2n} &= (10^2)^n \equiv 1^n \equiv 1 \pmod{99}, \\ 10^{2n+1} &= 10 \times 10^{2n} \equiv 10 \pmod{99}. \end{aligned}$$

(ii) Let

$$\begin{aligned} N &= a_m a_{m-1} \dots a_2 a_1 a_0 \\ &= a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \dots + a_{m-1} 10^{m-1} + a_m 10^m \\ &= (10a_1 + a_0) + 10^2(10a_3 + a_2) + 10^4(10a_5 + a_4) + \dots \end{aligned}$$

Utilising the fact that $10^{2n} \equiv 1 \pmod{99}$, we have

$$N \equiv (10a_1 + a_0) + (10a_3 + a_2) + (10a_5 + a_4) + \dots \pmod{99},$$

and the remainder on dividing by 99 can be obtained from this sum of pairs of digits.

(iii) Working modulo 101, the successive powers of 10 are

$$10^0 \equiv 1, 10^1 \equiv 10, 10^2 \equiv -1, 10^3 \equiv -10, 10^4 \equiv 1, 10^5 \equiv 10, \text{ etc.}$$

Hence

$$\begin{aligned} N &= a_m a_{m-1} \dots a_2 a_1 a_0 \\ &= a_0 + a_1 10 + a_2 10^2 + a_3 10^3 + \dots + a_{m-1} 10^{m-1} + a_m 10^m \\ &\equiv (10a_1 + a_0) - (10a_3 + a_2) + (10a_5 + a_4) - \dots \pmod{101}, \end{aligned}$$

and the remainder on dividing by 101 is obtained from this alternating sum of pairs of digits. Now

$$\begin{aligned} 62479 &\equiv 79 - 24 + 6 = 61 \pmod{101} \text{ and} \\ 9850833 &\equiv 33 - 8 + 85 - 9 = 101 \equiv 0 \pmod{101}, \end{aligned}$$

so the remainders are 61 and 0 respectively.

The last term in the summation is $10^{m-1}(10a_m + a_{m-1})$ if m is odd and $10^m(0 + a_m)$ if m is even.

Solution to Exercise 3.1

(a) We evaluate $P_1(x)$ for each of the least positive residues modulo 7, namely $x = 0, 1, 2, 3, 4, 5$ and 6.

$$\begin{aligned} 0^2 + 3 \times 0 + 4 &= 4 \equiv 4 \pmod{7} \\ 1^2 + 3 \times 1 + 4 &= 8 \equiv 1 \pmod{7} \\ 2^2 + 3 \times 2 + 4 &= 14 \equiv 0 \pmod{7} \\ 3^2 + 3 \times 3 + 4 &= 22 \equiv 1 \pmod{7} \\ 4^2 + 3 \times 4 + 4 &= 32 \equiv 4 \pmod{7} \\ 5^2 + 3 \times 5 + 4 &= 44 \equiv 2 \pmod{7} \\ 6^2 + 3 \times 6 + 4 &= 58 \equiv 2 \pmod{7} \end{aligned}$$

So $P_1(x) \equiv 0 \pmod{7}$ has the one solution $x \equiv 2 \pmod{7}$.

- (b) We need to evaluate $P_2(x)$ on a complete set of residues. This time we choose the least absolute residues modulo 5, namely $x = -2, -1, 0, 1$ and 2 .

Note that the fact that $P(a) = P(-a)$ influences the use of the least absolute residues for, as you can see, it effectively reduces the number of residues to be checked.

$$P_2(0) = -1 \equiv 4 \pmod{5}$$

$$P_2(1) = P_2(-1) = 1 - 1 \equiv 0 \pmod{5}$$

$$P_2(2) = P_2(-2) = 16 - 1 \equiv 0 \pmod{5}$$

So $P_2(x) \equiv 0 \pmod{5}$ has the four solutions $x \equiv 1, 2, -2$ and $-1 \pmod{5}$. That is, alternatively, $x \equiv 1, 2, 3$ and $4 \pmod{5}$.

Solution to Exercise 3.2

- (a) Since $\text{hcf}(5, 10) = 5$ and 5 does not divide 13, this congruence has *no* solutions.
- (b) Since $\text{hcf}(5, 13) = 1$, this congruence has a *unique* solution.
- (c) Since $\text{hcf}(10, 30) = 10$ and 10 does not divide 5, this congruence has *no* solutions.
- (d) Since $\text{hcf}(27, 24) = 3$ and 3 divides 318, this congruence has *three* solutions.

Solution to Exercise 3.3

- (a) The congruence has a unique solution modulo 53.

$$\begin{aligned} 28x &\equiv 49 \pmod{53} \iff 4x \equiv 7 \pmod{53} && \text{step 3} \\ &\iff 4x \equiv 60 \pmod{53} && \text{step 4} \\ &\iff x \equiv 15 \pmod{53} && \text{step 3} \end{aligned}$$

- (b) $\text{hcf}(34, 52) = 2$ and 2 does not divide 19, so the congruence has no solutions.

- (c) The congruence has a unique solution modulo 19.

$$\begin{aligned} 137x &\equiv 96 \pmod{19} \iff 4x \equiv 1 \pmod{19} && \text{step 4} \\ &\iff 4x \equiv 20 \pmod{19} && \text{step 4} \\ &\iff x \equiv 5 \pmod{19} && \text{step 3} \end{aligned}$$

- (d) The congruence has a unique solution modulo 53.

$$\begin{aligned} 51x &\equiv 8 \pmod{53} \iff -2x \equiv 8 \pmod{53} && \text{step 4} \\ &\iff 2x \equiv -8 \pmod{53} && \text{step 5} \\ &\iff x \equiv -4 \pmod{53} && \text{step 3} \\ &\iff x \equiv 49 \pmod{53} && \text{step 4} \end{aligned}$$

$137 \equiv 4 \pmod{19}$ and
 $96 \equiv 1 \pmod{19}$.

Rather than multiply through by -1 and then divide by 2 we could simply divide through by -2 .

- (e) As $\text{hcf}(18, 69) = 3$ and 3 divides 39, this congruence has three solutions modulo 69.

$$\begin{aligned}
 18x \equiv 39 \pmod{69} &\iff 6x \equiv 13 \pmod{23} && \text{step 2} \\
 &\iff 6x \equiv 36 \pmod{23} && \text{step 4} \\
 &\iff x \equiv 6 \pmod{23} && \text{step 3} \\
 &\iff x \equiv 6, 29, 52 \pmod{69}
 \end{aligned}$$

The final step gives the derived solution in terms of the original modulus.

We still use the equivalence symbol $\iff$ despite the different moduli, because an integer x is a solution of the previous congruence if, and only if, it is a solution of the following congruence.

Solution to Exercise 3.4

- (a) (i) $8x \equiv 12 \pmod{60} \iff 2x \equiv 3 \pmod{15}$
 $\iff 2x \equiv 18 \pmod{15}$
 $\iff x \equiv 9 \pmod{15}$
 $\iff x \equiv 9, 24, 39, 54 \pmod{60}$
- (ii) $21x \equiv 35 \pmod{47} \iff 3x \equiv 5 \pmod{47}$
 $\iff 3x \equiv -42 \pmod{47}$
 $\iff x \equiv -14 \equiv 33 \pmod{47}$
- (iii) $6x \equiv 5 \pmod{41} \iff 42x \equiv 35 \pmod{41}$
 $\iff x \equiv 35 \pmod{41}$
- (iv) $5x \equiv 1 \pmod{93} \iff 95x \equiv 19 \pmod{93}$
 $\iff 2x \equiv 112 \pmod{93}$
 $\iff x \equiv 56 \pmod{93}$

- (b) (i) Working modulo 7 gives

$$0^3 \equiv 0, 1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv 6, 4^3 \equiv 1, 5^3 \equiv 6 \text{ and } 6^3 \equiv 6.$$

Therefore the equation $x^3 \equiv 1 \pmod{7}$ has solutions $x \equiv 1, 2, 4 \pmod{7}$.

- (ii) The value of $2x^2 + 4x + 5 \pmod{7}$ for each of the seven values of x in a complete set of residues is given in the following table.

x	0	1	2	3	4	5	6
$2x^2 + 4x + 5$	5	4	0	0	4	5	3

Hence $2x^2 + 4x + 5 \equiv 0$ has the two solutions $x \equiv 2, 3 \pmod{7}$.

- (c) (i) The obvious moduli to try are 12 and 19 as each of these eliminates one of the variables.

Writing the equation as a congruence modulo 12 gives

$$19y \equiv 7 \pmod{12},$$

which on replacing 19 by the congruent number 7 simplifies to

$$y \equiv 1 \pmod{12}.$$

Substituting $y = 1$ into the original equation gives $x = -1$, and so the general solution is

$$x = -1 + 19k, \quad y = 1 - 12k, \quad k \in \mathbb{Z}.$$

- (ii) Writing the equation modulo 17 we have

$$\begin{aligned} 41y &\equiv 13 \pmod{17} \iff 7y \equiv 13 \pmod{17} \\ &\iff 35y \equiv 65 \pmod{17} \quad \text{multiplying by 5} \\ &\iff y \equiv 14 \equiv -3 \pmod{17}. \end{aligned}$$

Substituting $y = -3$ into the original equation gives $x = 8$, and hence the general solution is

$$x = 8 + 41k, \quad y = -3 - 17k, \quad k \in \mathbb{Z}.$$

- (d) Take the uniqueness first. The congruence $ax \equiv b \pmod{20}$ has a unique solution if, and only if, $\text{hcf}(a, 20) = 1$; that is, when $a = 1, 3, 7, 9, 11, 13, 17$ and 19 . For each of these eight values of a there are twenty values of b , making 160 congruences in total for which the solution is unique.

The congruence has $\text{hcf}(a, 20)$ solutions whenever $\text{hcf}(a, 20)$ divides b . So consider the possible values of $\text{hcf}(a, 20)$ in turn.

$\text{hcf}(a, 20) = 1$ leads to 160 solvable congruences, as already seen.

$\text{hcf}(a, 20) = 2$ when $a = 2, 6, 14$ and 18 . For each of these four values of a the congruence is solvable provided b takes one of the ten even values $0, 2, 4, 6, 8, 10, 12, 14, 16$ or 18 . Hence there are 40 congruences with solutions.

$\text{hcf}(a, 20) = 4$ when $a = 4, 8, 12$ and 16 . For each of these four values of a the congruence has solutions when b takes one of the five values $0, 4, 8, 12$ or 16 , making 20 congruences in all.

$\text{hcf}(a, 20) = 5$ when $a = 5$ or 15 . For each of these two values of a the congruence has solutions if b takes one of the values $0, 5, 10$ or 15 , making 8 congruences in all.

$\text{hcf}(a, 20) = 10$ when $a = 10$. In this case the congruence is solvable when $b = 0$ or 10 , making 2 congruences in all.

Altogether there are 230 congruences that have solutions.

You might like to compare this approach with that used in Subsection 5.2 of Chapter 1.

Solution to Exercise 4.1

Expressed in terms of congruence, the three conditions to be satisfied are

$$2n + 3 \equiv 0 \pmod{9}; \quad 3n + 4 \equiv 0 \pmod{16}; \quad 4n + 5 \equiv 0 \pmod{25}.$$

Solving these individually gives the equivalent system

$$n \equiv 3 \pmod{9}; \quad n \equiv 4 \pmod{16}; \quad n \equiv 5 \pmod{25},$$

as, for example,

$$\begin{aligned} 2n + 3 \equiv 0 \pmod{9} &\iff 2n \equiv -3 \pmod{9} \iff 2n \equiv 6 \pmod{9} \\ &\iff n \equiv 3 \pmod{9}. \end{aligned}$$

The variables in the proof of the Chinese Remainder Theorem are

$$b_1 = 3, \quad b_2 = 4, \quad b_3 = 5, \quad n_1 = 9, \quad n_2 = 16, \quad n_3 = 25, \quad N = 3600, \\ N_1 = 400, \quad N_2 = 225, \quad N_3 = 144.$$

$$\begin{aligned} N_1x = 400x \equiv 1 \pmod{9} &\iff 4x \equiv 1 \pmod{9} \\ &\iff x \equiv 7 \pmod{9}, \text{ so } x_1 = 7. \\ N_2x = 225x \equiv 1 \pmod{16} &\iff x \equiv 1 \pmod{16}, \text{ so } x_2 = 1. \\ N_3x = 144x \equiv 1 \pmod{25} &\iff 19x \equiv 1 \equiv 76 \pmod{25} \\ &\iff x \equiv 4 \pmod{25}, \text{ so } x_3 = 4. \end{aligned}$$

Therefore

$$x_0 = 3 \times 400 \times 7 + 4 \times 225 \times 1 + 5 \times 144 \times 4 = 12\,180 \equiv 1380 \pmod{3600}$$

and the least positive solution is $n = 1380$.

Solution to Exercise 4.2

As $165 = 3 \times 5 \times 11$, we begin by solving the linear congruence to each of the moduli 3, 5 and 11.

$$\begin{aligned} 7x \equiv 9 \pmod{3} &\iff x \equiv 0 \pmod{3} \\ 7x \equiv 9 \pmod{5} &\iff x \equiv 2 \pmod{5} \\ 7x \equiv 9 \pmod{11} &\iff x \equiv 6 \pmod{11} \end{aligned}$$

Our task is now to solve the three congruences on the right-hand side simultaneously.

$$x \equiv 6 \pmod{11} \implies x = 6, 17, \dots,$$

increasing in steps of 11 until we reach a solution of the second congruence.

$$x \equiv 2 \pmod{5} \implies x = 17, 72, \dots,$$

increasing in steps of $11 \times 5 = 55$ until we reach a solution of the remaining congruence.

$$x \equiv 0 \pmod{3} \implies x \equiv 72 \pmod{11 \times 5 \times 3}.$$

Hence

$$x \equiv 72 \pmod{165}$$

is the unique solution of the congruence.

Solution to Exercise 4.3

(a) This system has no solutions since $\text{hcf}(12, 18) = 6$ and 6 does not divide $11 - 7 = 4$.

(b) This system has solutions since $\text{hcf}(12, 18)$ divides $10 - 4$, $\text{hcf}(7, 12) = 1$ (which divides all integers) and $\text{hcf}(7, 18) = 1$.

$$x \equiv 10 \pmod{18} \implies x = 10, 28, \dots,$$

$$x \equiv 4 \pmod{12} \implies x = 28, 64, 100, 136, \dots,$$

increasing in steps of $\text{lcm}(12, 18) = 36$,

$$x \equiv 3 \pmod{7} \implies x \equiv 136, 388, 640, \dots,$$

increasing in steps of $7 \times 36 = 252$.

The solution $x \equiv 136 \pmod{252}$ is unique.

Solution to Exercise 4.4

(a) Following the proof of the Chinese Remainder Theorem, the variables are $n_1 = 4$, $n_2 = 5$, $n_3 = 7$, $N = 4 \times 5 \times 7 = 140$, $N_1 = 35$, $N_2 = 28$, $N_3 = 20$, $b_1 = 1$, $b_2 = 3$, $b_3 = 0$.

$$N_1 x_1 \equiv 1 \pmod{n_1} \iff 35x_1 \equiv 1 \pmod{4}$$

$$\iff 3x_1 \equiv 1 \pmod{4}, \text{ so } x_1 = 3.$$

$$N_2 x_2 \equiv 1 \pmod{n_2} \iff 28x_2 \equiv 1 \pmod{5}$$

$$\iff 3x_2 \equiv 1 \pmod{5}, \text{ so } x_2 = 2.$$

$$N_3 x_3 \equiv 1 \pmod{n_3} \iff 20x_3 \equiv 1 \pmod{7}$$

$$\iff -1x_3 \equiv 1 \pmod{7}, \text{ so } x_3 = 6.$$

The solution is

$$x_0 \equiv 1 \times 35 \times 3 + 3 \times 28 \times 2 + 0 \times 20 \times 6 = 273 \equiv 133 \pmod{140}.$$

The smallest natural number solution is 133.

(b) (i) We first solve the three congruences individually.

$$2x \equiv 3 \pmod{5} \iff x \equiv 4 \pmod{5}$$

$$3x \equiv 4 \pmod{7} \iff x \equiv 6 \pmod{7}$$

$$4x \equiv 9 \pmod{11} \iff x \equiv 5 \pmod{11}$$

Now,

$$x \equiv 5 \pmod{11} \implies x = 5, 16, 27, \dots,$$

increasing by 11 to a solution of the second congruence,

$$x \equiv 6 \pmod{7} \implies x = 27, 104, \dots,$$

increasing by $11 \times 7 = 77$ to a solution of the
congruence remaining,

and

$$x \equiv 4 \pmod{5} \implies x \equiv 104 \pmod{385}.$$

- (ii) As the moduli are not pairwise coprime, a little more care must be taken with this one.

$x \equiv 1 \pmod{4}$ and $x \equiv 3 \pmod{6}$ have a unique simultaneous solution modulo 12 (the least common multiple of 4 and 6), since $\text{hcf}(4, 6) = 2$ divides the difference $3 - 1$. By inspection this solution is $x \equiv 9 \pmod{12}$.

$x \equiv 9 \pmod{12}$ and $x \equiv 3 \pmod{9}$ have a unique simultaneous solution modulo 36 (the least common multiple of 12 and 9), since $\text{hcf}(12, 9) = 3$ divides the difference $9 - 3$.

$$x \equiv 9 \pmod{12} \implies x = 9, 21, \dots,$$

and

$$x \equiv 3 \pmod{9} \implies x \equiv 21 \pmod{36}.$$

- (c) $2310 = 2 \times 3 \times 5 \times 7 \times 11$ and so we require the simultaneous solution of the system

$$19x \equiv 7 \pmod{2}; \quad 19x \equiv 7 \pmod{3}; \quad 19x \equiv 7 \pmod{5};$$

$$19x \equiv 7 \pmod{7}; \quad 19x \equiv 7 \pmod{11}.$$

Solving these individually gives the equivalent system

$$x \equiv 1 \pmod{2}; \quad x \equiv 1 \pmod{3}; \quad x \equiv 3 \pmod{5};$$

$$x \equiv 0 \pmod{7}; \quad x \equiv 5 \pmod{11}.$$

Now

$$x \equiv 1 \pmod{2} \implies x = 1, \dots, \quad \text{increasing in steps of 2,}$$

$$x \equiv 1 \pmod{3} \implies x = 1, 7, 13, \dots, \quad \text{increasing in steps of 6,}$$

$$x \equiv 3 \pmod{5} \implies x = 13, 43, 73, 103, 133, \dots, \quad \text{increasing in steps of 30,}$$

$$x \equiv 0 \pmod{7} \implies x = 133, 343, 553, 763, 973, \dots, \quad \text{increasing in steps of 210.}$$

The order in which the individual congruences are incorporated does not matter. We have usually started with the one with largest modulus, but here we have chosen the opposite order.

Finally,

$$x \equiv 5 \pmod{11} \implies x \equiv 973 \pmod{2310}.$$

- (d) Translated into a problem in simultaneous congruences, we have to solve the system

$$n \equiv 0 \pmod{9}; \quad n \equiv 15 \pmod{16}; \quad n \equiv 23 \pmod{25}.$$

Now

$$n \equiv 23 \pmod{25} \implies n = 23, 48, 73, 98, 123, 148, 173, 198, 223, \dots, \quad \text{increasing in steps of 25,}$$

$$n \equiv 15 \pmod{16} \implies n = 223, 623, 1023, 1423, 1823, 2223, \dots, \quad \text{increasing in steps of } 16 \times 25 = 400.$$

Finally

$$n \equiv 0 \pmod{9} \implies n \equiv 2223 \pmod{3600}.$$

- (e) The arithmetic progression comprises numbers of the form $11k + 7$, and so three consecutive terms of the sequence are $11n + 7$, $11n + 18$ and $11n + 29$. Our task is therefore to solve, for n , the system of linear congruences

$$11n + 7 \equiv 0 \pmod{2}; \quad 11n + 18 \equiv 0 \pmod{3}; \quad 11n + 29 \equiv 0 \pmod{5},$$

which, after simplification, becomes

$$n \equiv 1 \pmod{2}; \quad n \equiv 0 \pmod{3}; \quad n \equiv 1 \pmod{5}.$$

The first and third of these congruences require that $n \equiv 1 \pmod{10}$, so

$$n = 1, 11, 21, \dots$$

The first number in this sequence to satisfy the remaining congruence, $n \equiv 0 \pmod{3}$, is $n = 21$. The three numbers in the arithmetic sequence are therefore 238, 249 and 260.

- (f) To be in a position to apply Theorem 4.5 we must first solve each individual congruence.

$$5x \equiv c \pmod{12} \iff 25x \equiv 5c \pmod{12} \iff x \equiv 5c \pmod{12}$$

$$7x \equiv 2 \pmod{30} \iff 7x \equiv -28 \pmod{30} \iff x \equiv -4 \equiv 26 \pmod{30}$$

The system has solutions when $\text{hcf}(12, 30)$ divides $26 - 5c$; that is, when 6 divides $26 - 5c$.

$$5c \equiv 26 \pmod{6} \iff 5c \equiv 20 \pmod{6} \iff c \equiv 4 \pmod{6}$$

So the system has a simultaneous solution when $c \equiv 4 \pmod{6}$.

- (g) The number of gold coins n satisfies each of the congruences

$$n \equiv 4 \pmod{17}; \quad n \equiv 10 \pmod{16}; \quad n \equiv 0 \pmod{15}.$$

Now

$$n \equiv 4 \pmod{17} \implies n = 4, 21, 38, 55, 72, 89, 106, \dots,$$

$$n \equiv 10 \pmod{16} \implies n = 106, 378, 650, 922, 1194, 1466, 1738, 2010, \dots,$$

increasing in steps of $16 \times 17 = 272$,

and

$$n \equiv 0 \pmod{15} \implies n \equiv 2010 \pmod{15 \times 16 \times 17}.$$

The least possible number of coins is 2010.